الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة الحاج لخضر. باتنة

كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية

قسم: العلوم الإسلامية

تخصص: فقه وأصول

نيابة العمادة لما بعد التدرج

والبحث العلمي والعلاقات الخارجية

الجـريمـة الإلكترونيـة في الفقه الجنائي الإسلامي

ـ دراسة مقارنة ـ

أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الفقه والأصول

إعـــداد الطالـــب:

أحمد أمدّاح

إشراف الأستاذ الدكتور

صالح بوبشيش

الاسم واللقب	الدرجة العلمية	الجامعة الأصلية	الصفة
مسعود فلوسي	أستـــاذ	جامعة باتنة	رئيسا
صالح بوبشيش	أستـــاذ	جامعة باتنة	مشرفا
كمال لدرع	أستـــاذ	جامعة الأمير قسنطينة	عضوا مناقشا
نور الدين بوحمزة	أستـــاذ	جامعة الجزائر 1	عضوا مناقشا
وسيلة خلفي	أستاذ محاضر (أ)	جامعة الجزائر 1	عضوا مناقشا
رشيد درغال	أستاذ محاضر (أ)	جامعة باتنة	عضوا مناقشا

السنة الجامعية

2014 م ـ 2015 م / 1435هـ ـ 1436هـ

إهداء

إلى الوالدين الكريمين؛ أدام الله عمرهما

إلى رفيقة دربي زوجتي حفظها الله،

إلى أبنائي الذين زاحمهم هذا البحث شيئا من حقوقهم،

إلى روح الأستاذ الشهيد الطاهر حليس طيب الله ثراه،

إلى روح المجاهد الرمز العقيد الحاج لخضر تغمده الله برحمته

وأسكنه فسيح جنانه

إلى إخواني جميعا، الذين أحاطوني بالعون والحب والدعاء

أهدي هذا البحث،

إن الحمد لله والشكر على ما منه عليّ من قوة العزيمة، وطول الصبر على مشاق البحث ومتاعبه، فلولا فضله سبحانه وتعالى لما انتهى بحثي بهذا لشكل.

وإذا كان من شكر بعد الله سبحانه وتعالى فهو لأستاذي القدير الأستاذ الدكتور صالح بوبشيش الذي تكرم بقبول الإشراف على هذه الأطروحة، فبذل النصح والإرشاد والتوجيه والتقويم ما أضاء لي طريق البحث كلما أحسست بانسداد في أفقه، أو صعوبة في مسلكه، فله جزيل الشكر والتقدير على ما خصني به من رعاية، وأسأل الله أن يمده بالصحة والعافية وأن يجعله نبراسا للعارفين.

ولا يفوتني أن أشكر كل الذين كان لهم دور في إعانتي على إنجاز هذا البحث، والذين لم يتوانوا في حثي ودفعي على مواصلة البحث وإنجازه.

مُقَدِّمَة

الحمد لله الذي خلق الإنسان من عدم وعلّمه ما لم يعلم ورغّبه في العلمِ والتعلُّمْ، والصلاة والسلام على هادي البشرية ومعلّم الإنسانية الذي أُمِرَ بالقراءة في أول آية أنزلت عليه والذي رغّب في التعلّمْ وحثّ عليه، أمَّا بعد:

قال تعالى: ﴿ إِنَّهُۥ مَن يَأۡتِ رَبَّهُۥ مُجۡرِمٗا فَإِنَّ لَهُۥ جَهَنَّمَ لَا يَمُوتُ فِيهَا وَلَا يَحۡيَىٰ ٧٤ ﴾[1]

إن الجريمة ظاهرة اجتماعية عامة لازمت المجتمع البشري منذ نشأته، حيث يطلعنا القرآن الكريم بأول جريمة إنسانية وقعت على وجه الأرض عندما قتل قابيل أخاه هابيل ظلما وعدوانا فيقول الله تعالى: ﴿وَٱتۡلُ عَلَيۡهِمۡ نَبَأَ ٱبۡنَيۡ ءَادَمَ بِٱلۡحَقِّۘ إِذۡ قَرَّبَا قُرۡبَانٗا فَتُقُبِّلَ مِنۡ أَحَدِهِمَا وَلَمۡ يُتَقَبَّلۡ مِنَ ٱلۡأٓخَرِۚ قَالَ لَأَقۡتُلَنَّكَۖ قَالَ إِنَّمَا يَتَقَبَّلُ ٱللَّهُ مِنَ ٱلۡمُتَّقِينَ ٢٧ لَئِنۢ بَسَطتَ إِلَيَّ يَدَكَ لِتَقۡتُلَنِي مَآ أَنَا۠ بِبَاسِطٖ يَدِيَ إِلَيۡكَ لِأَقۡتُلَكَۖ إِنِّيٓ أَخَافُ ٱللَّهَ رَبَّ ٱلۡعَٰلَمِينَ ٢٨ إِنِّيٓ أُرِيدُ أَن تَبُوٓأَ بِإِثۡمِي وَإِثۡمِكَ فَتَكُونَ مِنۡ أَصۡحَٰبِ ٱلنَّارِۚ وَذَٰلِكَ جَزَٰٓؤُاْ ٱلظَّٰلِمِينَ ٢٩ فَطَوَّعَتۡ لَهُۥ نَفۡسُهُۥ قَتۡلَ أَخِيهِ فَقَتَلَهُۥ فَأَصۡبَحَ مِنَ ٱلۡخَٰسِرِينَ ٣٠﴾[2]، ومنذ هذه الحادثة لزمت الجريمة المجتمعات قديمها وحديثها متأثرة بكافة المعطيات المحيطة بها، ولا يزال المجرمون يكيفون جرائمهم وفقا لبيئتهم ويزدادون مكرا وخطورة كلما ازدادت الأمة تطورا ونباهة، وهاهم الآن يحاولون الاستفادة من التقدم التقني في عصر ثورة المعلومات والتكنولوجيا المتطورة، حيث ظهرت أنماط جديدة من الجرائم لم تكن معهودة في السابق.

ففي منتصف القرن الثامن عشر ظهرت مرحلة جديدة في تاريخ الحضارة الإنسانية عرفت بثورة المعلومات والتكنولوجيا التي اكتسحت كل جوانب الحياة وأصبح العالم مرتبطا بعضه ببعض وكأنه قرية صغيرة ألغت معها الحدود الجغرافية والسياسية للدول، فتغير مفهوم الصراع بين الدول من التنافس نحو التسلح إلى التنافس حول امتلاك المعرفة، وأصبحت المعلومات هي المقياس الذي يقاس به

---

[1] ـــ سورة طه، الآية: 74.

[2] ـــ سورة المائدة، الآيات: 27-30.

قوة الشعوب وهي السلاح الذي يفصل بين القوة والضعف وبين النجاح والخسارة فمن يعلم ينتصر ومن لا يعلم سيكون مآله الهزيمة، وقد قال تعالى: ﴿قُلْ هَلْ يَسْتَوِي ٱلَّذِينَ يَعْلَمُونَ وَٱلَّذِينَ لَا يَعْلَمُونَ﴾[1].

وكنتيجة لهذه الثورة وما نجم عنها من تحولات اقتصادية واجتماعية تزايد استخدام الحاسوب كأداة لتخزين المعلومات ومعالجتها واسترجاعها، وكوسيلة لا يستغنى عنها في عمليات التصميم والتصنيع والإدارة، وبذلك تطورت تطبيقاته من إدارة بعض العمليات الحسابية إلى الخدمات في شتى المجالات وهو ما أدى إلى زيادة أهمية المعلومات، كما أصبح مألوفا استخدام شبكات المعلومات المحلية والإقليمية والعالمية بغرض الاستفادة المثلى من المعلومات في مختلف متطلبات الحياة البشرية المعاصرة.

وفي خضم تطور عالم المعلومات برز مجرمون يتمتعون بالخبرة والحرفية في تطويع التقنية للقيام بأعمال إجرامية لم تعهدها الإنسانية من قبل، فأصبح بإمكانهم الوصول إلى أي هدف يرغبون فيه عبر الإبحار في الشبكة المعلوماتية التي لا مكان ولا زمان يستطيع وضع حدود لها، وهو ما أدى إلى ظهور أنماط جديدة من الإجرام لم تكن مألوفة في السابق كالدخول غير المشروع إلى شبكات الحواسيب ونظم المعلومات، والتحايل على نظم المعالجة الآلية للبيانات، ونشر الفيروسات، وإتلاف البرامج وتزوير المحررات الإلكترونية، والتجسس الالكتروني، والإرهاب الالكتروني، ومهاجمة المراكز المالية والبنوك والحكومات الإلكترونية،كما تعدى الأمر أيضا إلى ظهور أنماط جديدة من الحروب التي أصبحت تعرف بالحروب الإلكترونية.

وإدراكا بمدى خطورة هذه الأعمال الإجرامية أصبحت مكافحتها من أولويات المجتمع الدولي والحكومات وذلك عن طريق سن التشريعات والأنظمة المكافحة لها، إلا أن هذه الظاهرة أثارت مشكلات قانونية عديدة من بينها؛ مجال الاختصاص القضائي ومكان وزمان ارتكاب الجريمة خاصة وأنه يسهل على المجرم ارتكاب جريمة ما في مكان غير الذي يتواجد فيه أو الذي حصلت فيه نتائجه، إضافة إلى الخلاف الحاصل في تصنيف بعض التصرفات كجرائم أم لا، كما أن التشريعات الوضعية لم

---

[1] ـــ سورة الزمر، الآية: 9.

تتقدم بذات السرعة التي تتقدم بها التقنية الحديثة وهو ما جعل الجريمة الإلكترونية والمجرم المعلوماتي يسبقان بمراحل كثيرة خطوات المشرع الوضعي في هذا المجال.

ولا تزال الأيام القادمة حُبلى بكل جديد ولا نزال في بداية عصر الانفجار المعلوماتي، مما يعني ظهور المزيد من هذه الأنماط الجديدة والذي يتوجب معها تحرك العلماء بما فيهم علماء الشريعة الإسلامية من أجل سن الضوابط الشرعية في التعاملات الإلكترونية.

و نظرا لأن السواد الأعظم في الكرة الأرضية من حيث التعداد البشري والأيديولوجي هم المسلمون فلاشك أن سن القوانين والتشريعات المستمدة من الشريعة الإسلامية قد تضع الكثير من الحواجز أمام من يرتكب مثل هذه الجرائم خاصة من داخل البلاد الإسلامية، فالطبيعة البشرية في كل مكان معرضة، ولذلك يجب العمل على تفعيل الأنظمة الرادعة لتواكب مستجدات الجريمة المتطورة سواء من حيث التقنية أو التشريع.

ومن هنا جاءت أهمية إفراد دراسة علمية فقهية متخصصة تبين الجوانب الشرعية لظاهرة الجريمة الإلكترونية في الفقه الجنائي الإسلامي، كمحاولة مني لإلقاء الضوء على حجم ونمط أبرز الجرائم المستحدثة وتحديدها قدر الإمكان مع بيان مدى خطورتها على المصالح العامة والخاصة، وهذا بغرض المساهمة في وضع الخطوط العريضة للتعرف على كيفية مكافحتها والحد منها بالاستناد إلى نصوص الشريعة الإسلامية التي لا تفتقر إلا لبذل المزيد من الاجتهاد على بصيرة والحضور الدائم عند كل طارئ واكتشاف الخصوصية لكل زمان ومكان وتقدير المناسب لهما من الأحكام والإجراءات والتدابير، مع التنويه سلفا بأنه لا يمكن حصر هذه الجرائم لسبب بسيط هو أن الجريمة الإلكترونية وأنماطها في تجدد مستمر ولا تقف إطلاقا عند أنماط محددة أو أشكال معينة.

إشكالية الدراسة:

لقد أصبحت تقنية المعلومات ووسائل الاتصال الحديثة جزءا من منظومة القيم والسلوك الإنساني لجميع أفراد المجتمع بما في ذلك المجتمع الإسلامي، كما أصبح استخدام التقنية من متطلبات الحياة ومؤشرا على الوعي الاجتماعي حيث تتيح خيارات أوسع في التعامل مع الواقع المعاش في كافة مجالات الحياة. لكن ما يثير القلق هو سرعة انتشارها مع عدم التحكم فيها وسوء استخدامها في كثير من الحالات وذلك في ظل غياب الوازع الديني والتوجيه الفعال لتجاوز الآثار السلبية لها، وهو ما نتج عنه ظهور سلوكيات منحرفة من خلال إساءة استخدام التقنيات الحديثة وعلى رأسها الحواسيب والانترنت والتي أثرت بدورها على المنظومة الأمنية في المجتمع.

وتعود المشكلة في ذلك أن التغيرات المادية السريعة لم يصاحبها في المجتمعات تغيرات القيم بنفس السرعة، بمعنى أن التطور المادي لم يصاحبه تطور في القيم التربوية يتناسب مع طبيعة التغير المادي السريع، وهو ما أحدث فجوة خلقية ما بين التطور المادي والتطور القيمي، فنتج عن ذلك ظهور ما يعرف بالثقافة الهامشية التي تهدف في الغالب إلى التنصل من القيم الأصلية واعتماد قيم وأخلاق بديلة، ولذلك أصبح المجتمع الإسلامي يعايش الكثير من الظواهر السلبية التي أفرزتها التقنية الحديثة لا تمد بصلة بالآداب والتصرفات الإسلامية، وعلى رأسها الجرائم الإلكترونية وما تحمله من مخاطر على الفرد والمجتمع والنظام العام.

وعلى ضوء ذلك فإن مشكلة الدراسة تنحصر في بيان حجم وأنماط الجرائم الإلكترونية بين مستخدمي الحواسيب والانترنت في المجتمع الإسلامي خاصة، مع تحديد أهم سمات وخصائص مرتكبي تلك الجرائم وهذا للوقوف على حجم خطورة الظاهرة ومن ثم بيان أحكامها في الشريعة الإسلامية، وذلك من خلال طرح التساؤل التالي:

ما التكييف الفقهي للجرائم الإلكترونية، وما عقوباتها الشرعية؟

وسأحاول الجواب على هذا السؤال من خلال الإجابة على التساؤلات التالية:

1 ــ ما المقصود بالجريمة الإلكترونية ؟ والمجرم المعلوماتي ؟ ومن هم المجني عليهم ؟ وما العوامل المؤثرة في وقوعهم ضحية للجريمة الإلكترونية ؟ وما موقف الفقه الإسلامي منها ؟

2 ــ ما هي أركان الجريمة الإلكترونية؟

3 ـــ ما أوجه الشبه بين الجريمة الإلكترونية والجريمة التقليدية ؟

4 ـــ ما هي الأساليب المستخدمة في الجرائم الإلكترونية ؟

5 ـــ ما صور الجرائم الإلكترونية ؟ وما الإجراءات الوضعية المتخذة لمواجهتها ؟ وما أوجه قصورها ؟

6 ـــ ما الذي يمكن استخلاصه من هذه الدراسة من نتائج ؟ وما الذي يمكن أن تتمخض عنه من توصيات ؟

أهمية الدراسة:

لقد ساهمت عدة أسباب وعوامل على جعل الجرائم الإلكترونية ظاهرة بالغة الخطورة على أمن المجتمع الدولي بوجه عام والمجتمع الإسلامي خاصة، الأمر الذي أدى إلى أهمية التعاون الدولي للتصدي لهذه الظاهرة الخطيرة والبحث في الوسائل الوقائية لإجهاض هذا النوع من الجرائم قبل وقوعها، خاصة وأن الحاسوب والانترنت قد صارا وسائط عالمية للتعامل بين الدول والشركات والأشخاص ويمثلان حاليا البنية الأساسية لكل المرافق التي تدار بالحاسوب بحيث أصبح عدم التعامل معهما خروجا من الدائرة الدولية.

ومن هنا تتبين أهمية التعرض لموضوع الجرائم الإلكترونية إذ أن احتمالات تعرض الأشخاص أو المؤسسات أو حتى الحكومات لجريمة إلكترونية صارت مرتفعة جدا، ودليل ذلك حجم الجرائم الإلكترونية مقارنة بالجريمة التقليدية مما يقودنا إلى إدراك عمق تأثيرها السلبي على المجتمع، خاصة وأن تكنولوجيا المعلومات والاتصالات أصبحت تأخذ حيزا مهما في التعاملات وصار الحاسوب هو محور كل التعاملات العامة والخاصة، وعلى الرغم مما تمثله هذه التقنية من تقدم إيجابي ومساهمة في تطوير أنماط الحياة، فإنها بالمقابل ساهمت في ابتكار طرق ووسائل أشد خطورة لارتكاب الجرائم بوسائل إلكترونية.

أسباب اختيار الموضوع:

من أهم الأسباب التي دفعتني لاختيار هذا الموضوع ما يلي:

1 ــ جدة الموضوع وحداثته، كون الجريمة الإلكترونية من الجرائم المستحدثة التي لم تحظ ببحوث ودراسات من الوجهة الشرعية مقارنة مع الجرائم التقليدية، ولذلك فهي بحاجة إلى دراسات معمقة لتقديم أجوبة ملائمة لهذه الظاهرة.

2 ــ استفحال ظاهرة الجرائم الإلكترونية وما أفرزته من آثار سلبية في المجتمعات بصفة عامة والمجتمع الإسلامي على الخصوص.

3 ــ نقص الوعي الكافي في المجتمع الإسلامي المتعلق بخطورة الظاهرة.

4 ــ رغبتي في الكشف عن أنواع الجرائم الإلكترونية وتكييفها الفقهي، وتوضيح أوجه الشبه والاختلاف بينها وبين الجرائم التقليدية.

5 ــ الرغبة في معالجة الموضوع لتعلقه بدراستي السابقة في رسالة الماجستير التي كان عنوانها: "التجارة الإلكترونية من منظور الفقه الإسلامي"، إضافة إلى الخبرة المكتسبة في مجال المعلوماتية، وتخصصي في الشريعة الإسلامية.

6 ــ رغبة مني في المساهمة بهذا الموضوع لإثراء المكتبة الجنائية الإسلامية، ودعم محاربة خطر الجريمة الإلكترونية.

7 ــ المساهمة في إحياء إحدى الفروض الغائبة عن الساحة الإسلامية اليوم، وعن جملة من قوالب الخطاب الديني، وهو فقه المصالح والمفاسد والمآلات؛ حيث ساهم غيابه ــ إلا ما ندَرَ ــ في ظهور الكثير من السلبيات التي تتنافى ومقاصد الشريعة الإسلامية.

8 ــ إبراز سمو الشريعة الإسلامية وشموليتها في معالجة ظاهرة الجريمة الإلكترونية بأساليب تحقق للمجتمع الأمن والاستقرار.

أهداف الدراسة:

إن بحث المواضيع المتعلقة بالجرائم الحدية أو التعزيرية، له قدر بالغ من الأهمية خاصة وأنها تتعلق بحفظ الضرورات الخمس التي يقوم على أساسها الدين الإسلامي، وقد جاءت الشريعة الإسلامية بما يقيم هذه الضرورات ويحفظها من الاختلال وهو ما أفاض به فقهاء الإسلام في هذا الجانب، ولا ريب أن معرفة كون الفعل جريمة أم لا، ومعرفة العقوبة المترتبة على ذلك يعود بالفائدة الكبيرة على الأفراد والمجتمع.

وبناء على ذلك فإن دراستي لموضوع الجريمة الإلكترونية تهدف إلى ما يلي:

1 ــ تعريف المجتمع الإسلامي بالجريمة الإلكترونية، والتحسيس بما تمثله هذه الجريمة من خطورة تهدد الأفراد والمجتمعات سواء على المستوى الوطني أو الإقليمي أو العالمي، وبالضرورة معرفة حجم الظاهرة في الواقع وبيان أبعادها ومدى خطورتها وأضرارها، وذلك من خلال دراسة أساليب الجريمة الإلكترونية وصورها وأنماطها.

2 ــ وتهدف الدراسة إلى بيان أهم سمات وخصائص مرتكبي الجريمة الإلكترونية وكذا حجم المجتمع المعلوماتي في الفضاء الإلكتروني مما يساعد في مواجهة الجريمة الإلكترونية والتعامل معها ومكافحتها، كما تهدف إلى لفت انتباه الباحثين في المجال الأمني والاجتماعي خاصة، إلى كثير من الظواهر السلوكية المتعلقة باستخدام الانترنت والتي تتطلب البحث والدراسة.

3 ــ لفت انتباه المعنيين و المسؤولين عن الأجهزة والتنظيمات التربوية، والإعلامية، والشؤون الدينية، والمؤسسات العلمية، للمساهمة في مكافحة الجريمة الإلكترونية والحد منها، وتحذير أولياء الأمور وكافة شرائح المجتمع من التعامل معها وبيان عظيم خطرها.

4 ــ إلقاء الضوء على الجهود الفنية والتشريعات المقارنة تجاه الجريمة الإلكترونية وبيان مدى فاعلية هذه التشريعات في مواجهتها، وأوجه القصور الذي يعتريها.

5 ــ التوصل إلى مدى مشروعية الجرائم الإلكترونية وعقوباتها في الفقه الجنائي الإسلامي.

الدراسات السابقة:

لقد أسهب العلماء والباحثون في مجال المعلوماتية والجرائم الإلكترونية بنشر أعداد هائلة من الدراسات التي تعالج الظاهرة من الناحية التقنية والقانونية وأغلبها مؤلف باللغات الأجنبية، بينما الدراسات المتعلقة بالجريمة الإلكترونية من الناحية الفقهية فتكاد تنعدم حسب اطلاعي، حيث بحثت في العديد من مكتبات جامعات الدول العربية والمعارض المقامة بها كدولة الإمارات العربية المتحدة، والمملكة العربية السعودية، وجمهورية مصر العربية، والمملكة المغربية، والجمهورية التونسية، وما لاحظته أن أغلب المراجع العربية تعالج الجرائم الإلكترونية من وجهة التشريع الوضعي، كما تطرق البعض منها إلى ظاهرة السرقة الإلكترونية على وجه المقارنة بين الشريعة والقانون مع حصر الدراسة على المستوى المحلي لبلد المؤلف، إضافة إلى بعض المقالات المنشورة على المجلات أو المواقع الإلكترونية لكنها لا ترقى إلى المستوى المطلوب، ومن بين الدراسات ذات الصلة ما يلي:

ـــ "**جرائم الحاسب الآلي وعقوباتها في الفقه والنظام**":(جريمة استنساخ برامج الحاسب الآلي وبيعها، وإنتاج الفيروسات ونشرها)، لمحسن بن سليمان الخليفة.

وهي عبارة عن رسالة ماجستير مقدمة إلى أكاديمية نايف العربية للعلوم الأمنية، قسم العدالة الجنائية، الرياض، 1424هـ.

اشتملت الدراسة على مقدمة وتمهيد وثلاثة فصول، تطرق الفصل الأول منها إلى مفهوم الحاسب الآلي وشبكاته، ومفهوم جرائم الحاسب الآلي. وبحث الفصل الثاني جريمة استنساخ برامج الحاسب الآلي وبيعها وإنتاج الفيروسات في الفقه والقانون الوضعي، وتطرق الفصل الثالث إلى عقوبة استنساخ البرامج وإنتاج الفيروسات بين الفقه والقانون.

ـــ "**جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية**"، لبلال أمين زين الدين، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008م.

وهي عبارة عن دراسة مقارنة بين الشريعة والقانون بحث فيها المؤلف جريمة السرقة وخيانة الأمانة في إطار المعالجة الآلية للبيانات، وجريمة الدخول والبقاء في النظام المعلوماتي، واعتراض انتقال البيانات أو إتلافها أو تزويرها، لكن ما لاحظته أن المؤلف ركز كثيرا على الجانب الوضعي في معالجة

الظاهرة، بينما تكاد تخلو دراسته للظاهرة من الناحية الشرعية حيث اكتفى بذكر بعض الآيات القرآنية، وتطرق لمعاني بعض الأحاديث النبوية الشريفة دون تخريجها.

ـــ "**الجرائم الإلكترونية في الفقه الإسلامي والقوانين**"، لمحمد جلال، الطبعة الأولى ، مكتبة القانون والاقتصاد، القاهرة، مصر، جانفي 2015م.

تعرض المؤلف إلى العديد من صور الجرائم الإلكترونية من النظرة القانونية حيث استعان بعدد كبير من القوانين والتشريعات الدولية المقارنة، كما بين الحكم الشرعي في استخدام الحاسب الآلي أو الانترنت إذا ترتب على استعمالها مشاهدة أو سماع شيء من المحرمات أو استعين بهما على فعل شيء منها، والدخول إلى المواقع الإباحية أو بث الفتن ونشرها بين الناس، والقذف والتشهير، أو سرقة أموال الغير، أو تأخير الصلوات وتضييع الفرائض، وتوصل في دراسته إلى أن استخدام الحاسوب والانترنت بقصد الإضرار بالغير وبث الفساد الفكري أو الأخلاقي هو محرم في الشريعة الإسلامية استنادا إلى القاعدة الشرعية العامة " لا ضرر ولا ضرار".

أما الجديد الذي سيأتي به البحث هو دراسة فقهية حديثة متخصصة تتطابق وواقع الشريعة والفقه الإسلامي، أملا أن تساهم في دعم المكتبة الإسلامية وأن تكون أرضية خصبة تساعد الباحثين في صلب الموضوع.

منهج الدراسة:

إن اعتماد منهج واحد في دراسة أي موضوع هو مدعاة لإهمال كثير من جوانب الموضوع والتركيز على جوانب معينة فيه، وهذا يفقد الدراسة توصلها إلى بعض النتائج المرجوة ويضعف خصوبتها، وبناء على ذلك فقد اعتمدت في دراستي للموضوع على عدد من المناهج:

1 ـــ المنهج الاستقرائي، الذي يعتمد على وصف الوقائع والظواهر لإدراك ما بينها من علاقات متبادلة، وتصنيف خصائصها وترتيبها واكتشاف الارتباط بينها، وهذا بغرض الكشف عن المعطيات الحسية لظاهرة الجريمة الإلكترونية على أساس الملاحظة والتجربة.

2 ــ المنهج التاريخي، الذي يقوم على فكرة استرداد خبرات البشرية الماضية، وما جرت عليه أحداث التاريخ للإنسان؛ بهدف دراسة ظواهر حاضرة من أجل فهمها والإفادة منها، فقمت بمراجعات سريعة لمفاهيم الظاهرة كالتطور التاريخي للحاسوب، والانترنت، و التطور التاريخي للجريمة الإلكترونية حتى صارت على النحو المعروف، بالإضافة إلى تطور التشريع الوضعي للظاهرة وكيف تميزت عن الجرائم التقليدية بعد مرور الزمن.

3 ــ المنهج الوصفي، ويقوم على دراسة الظاهرة كما هي موجودة في الواقع، عن طريق وصفها وصفا دقيقا؛ وذلك بدراسة خصائصها، وحجمها، حيث قمت بدراسة الجريمة الإلكترونية من حيث الخصائص والأركان والأساليب، كما قمت بدراسات مسحية للظاهرة من أجل جمع المعلومات والبيانات والإحصاءات بقصد التعريف على ماهية الجريمة الإلكترونية وحجم المخاطر التي تنطوي عليها.

4 ــ المنهج المقارن، الذي يقوم على المقارنة بين أنماط مختلفة من الظواهر والأحداث بهدف التعرف على العناصر الثابتة والعناصر المتغيرة بينها، وإظهار أوجه الاتفاق والاختلاف.. وقد استغللت معطيات هذا المنهج بدراسة مقارنة لعدد من الأحكام الشرعية بغرض مناقشة أدلتها أصوليا والموازنة بينها فيما يتعلق بالجرائم المستحدثة وترجيح الأقوى دليلا، أو الإتيان برأي جديد.

5 ــ المنهج التحليلي، وهو منهج لازم البحث في جميع مراحله بغرض الوصول إلى استنتاج أحكام شرعية تتعلق بظاهرة الجريمة الإلكترونية.

خطـــة البحث:

بعد توجهي إلى الله تعالى بالدعاء أن يلهمني الصواب في هذه النازلة، قمت بجمع المعلومات المتعلقة بموضوع البحث لمعرفة حقيقتها وأقسامها ونشأتها وأسباب ظهورها والظروف المحيطة بها، ثم اتصلت بأهل الاختصاص في موضوع البحث وأعددت لهذا الغرض مجموعة من الأسئلة للتأكد من المعلومات وإزالة ما يعترضني من إشكالات وملابسات وذلك عملا بقوله تعالى: ﴿فَسْـَٔلُوٓاْ أَهْلَ ٱلذِّكْرِ إِن كُنتُمْ لَا تَعْلَمُونَ﴾[1] ، وبناء على ذلك رسمت خطة البحث كما يلي:

---

[1] ــ سورة النحل، الآية: 43.

قسمت البحث إلى أربعة أبواب، تطرقت في الباب الأول إلى المفاهيم المتعلقة بالدراسة كمفهوم الجريمة الإلكترونية، ومفهوم الفقه الجنائي الإسلامي، كما بينت أدوات الجريمة الإلكترونية، ومفهوم المجرم المعلوماتي وسماته، وتطرقت إلى مصطلح المجتمع المعلوماتي ومؤشراته مستعينا بعلم الإحصاء لمعرفة حجمه في العالم الافتراضي.

وتطرقت في الباب الثاني إلى أنواع الجرائم الإلكترونية وآثارها، والأساليب المتخذة في ارتكاب هذا النوع من الجرائم تمهيدا لتخريج أحكامها في الباب التطبيقي.

أما الباب الثالث فقسمته إلى فصلين وضحت من خلالهما الجهود الدولية المبذولة في مواجهة الظاهرة ممثلة في الآليات الفنية والتشريعات القانونية المتخذة، بغرض التنويه إلى أن اختراق الحواسيب والشبكات عن طريق كسر أنظمة حمايتها القوية هو من باب انتهاك حرز الأنظمة، كما بينت مدى فاعلية الإجراءات التقنية والتشريعية تجاه الجريمة الإلكترونية حيث ثبت عدم صمودها خاصة منها التشريعات الوضعية نظرا لما تعانيه من قصور.

وفي الباب التطبيقي بيّنت المسؤولية الجنائية عن الجرائم الإلكترونية في الفقه الجنائي الإسلامي، وذلك عن طريق تشريح الجرائم الإلكترونية التي تم ذكرها وفق ضوابط الاجتهاد الإسلامي، كما أعدت تصنيفها حسب اجتهادي باعتبار الضرر الذي تلحقه بالمقاصد الشرعية في فصول ثلاثة.

وكانت خطة البحث كما يلي:

المقدمة

الباب الأول: مفاهيم الدراسة

الفصل الأول: مفهوم الجريمة الإلكترونية والفقه الجنائي الإسلامي

المبحث الأول: مفهوم الجريمة في اللغة والاصطلاح

المبحث الثاني: مفهوم الجريمة الالكترونية، خصائصها وأركانها

المبحث الثالث: مفهوم الفقه الجنائي الإسلامي

الفصل الثاني: أدوات الجريمة الالكترونية

المبحث الأول: الحاسوب، تعريفه، نشأته وأهميته

المبحث الثاني: شبكة المعلومات العالمية

الفصل الثالث: المجرم المعلوماتي وعلاقته بالجريمة الإلكترونية

المبحث الأول: المفهوم العام للمجرم وسيكولوجيته

المبحث الثاني: سمات المجرم المعلوماتي وتصنيفاته

المبحث الثالث: المجرم المعلوماتي والهندسة الاجتماعية

الفصل الرابع: المجتمع المعلوماتي ومؤشراته

المبحث الأول: مفهوم المجتمع المعلوماتي

المبحث الثاني: المؤشرات الإحصائية للمجتمع المعلوماتي

الباب الثاني: أنواع الجرائم الالكترونية وآثارها

الفصل الأول: الجرائم الإلكترونية المتعلقة بأمن المعلومات

المبحث الأول: الجرائم المستهدفة للحواسيب

المبحث الثاني: جرائم تطوير الفيروسات ونشرها

المبحث الثالث: جرائم تدمير المواقع الإلكترونية

المبحث الرابع: جرائم اختراق البريد الإلكتروني وقرصنة البرامج.

المبحث الخامس: جريمة التزوير الإلكتروني

الفصل الثاني: الجرائم الإلكترونية المتعلقة بالأموال والأشخاص

المبحث الأول: الجرائم الإلكترونية المتعلقة بالأموال

المبحث الثاني: الجرائم الإلكترونية المتعلقة بالأشخاص والآداب العامة

الفصل الثالث: الجرائم الإلكترونية المتعلقة بأمن الدول والمجتمعات

المبحث الأول: جرائم التجسس الإلكتروني

المبحث الثاني: الجريمة المنظمة عبر الانترنت.

المبحث الثالث:الإرهـــــاب الإلكتـــروني

الباب الثالث: الآليات الفنية والتشريعات القانونية لمكافحة الجريمة الإلكترونية

الفصل الأول: الإجراءات الفنية لمكافحة الجريمة الإلكترونية

المبحث الأول: مفهوم أمن المعلومات

المبحث الثاني: الوسائل التقنية لأمن المعلومات

المبحث الثالث:الحاسوب الجنائي ودوره في أمن المعلومات

الفصل الثاني: التدابير والتشريعات القانونية لمكافحة الجريمة الإلكترونية

المبحث الأول: مفهوم القانون الجنائي وصوره الجزائية

المبحث الثاني: التشريعات القانونية الإقليمية تجاه الجرائم الإلكترونية

المبحث الثالث: التدابير والمعاهدات الدولية لمكافحة الجرائم الإلكترونية

الباب الرابع: المسؤولية الجنائية عن الجرائم الإلكترونية في الفقه الجنائي الإسلامي

الفصل الأول: جرائم الاعتداء على المال وحكمها في الفقه الجنائي الإسلامي

المبحث الأول: جرائم التعدي على الحاسوب والبرامج

المبحث الثاني: جرائم التعدي على المواقع الإلكترونية

المبحث الثالث: جرائم التزوير الإلكتروني

المبحث الرابع: جرائم التعدي على النقود الإلكترونية

المبحث الخامس: جرائم التعدي على التجارة الإلكترونية

الفصل الثاني: جرائم الاعتداء على النفس والعرض وحكمها في الفقه الجنائي الإسلامي

المبحث الأول: القذف والتشهير الإلكتروني

المبحث الثاني: جرائم التعدي على البريد الإلكتروني

المبحث الثالث: جريمة صناعة المواقع الإباحية وترويجها عبر الانترنت

الفصل الثالث: جرائم الاعتداء على أمن الدولة والمجتمع وحكمها في الفقه الجنائي الإسلامي

المبحث الأول: جرائـــم التجسس الإلكتروني

المبحث الثاني: جريمة غسيل الأموال عن طريق الانترنت

المبحث الثالث: جرائم الإرهاب الإلكتروني

الخاتمة ونتائج البحث

التوصيات المقترحة

الباب الأول

مفاهيم الدراسة

الفصل الأول: مفهوم الجريمة الإلكترونية والفقه الجنائي الإسلامي

الفصل الثاني: أدوات الجريمة الإلكترونية

الفصل الثالث: المجرم المعلوماتي وعلاقته بالجريمة الإلكترونية

الفصل الرابع: المجتمع المعلوماتي ومؤشراته

1)
2)
..

تمهيد:

أبرزت الإحصاءات الحديثة أن مشكلة الجريمة في السنوات الأخيرة تزداد حدة يوما بعد يوم حيث تحمل في طياتها مخاطر كبيرة على مستوى بلدان العالم[1]، فإلى جانب هدرها للأنفس والأموال، والحقوق، والحريات، وإخلالها بأمن المجتمعات واستقرارها، فإن مكافحتها تشكل عبئا ثقيلا على الاقتصاد القومي[2].

ولإدراك مخاطر الجريمة الإلكترونية ومضارها فإنه من الضروري التطرق إلى مفاهيم الدراسة محل البحث، وهو ما سأدرسه من خلال هذا الباب الذي سأتطرق فيه إلى حقيقة الجريمة الإلكترونية والفقه الجنائي الإسلامي، كما سأبحث عن الأدوات والوسائل المادية والمعنوية التي تقوم على أساسها الجريمة الإلكترونية، والتعريف بالمجرم المعلوماتي من حيث سماته وتصنيفاته مقارنة بالمجرم الكلاسيكي مركزا في ذلك على أهم الطرق التي يعتمدها في استدراج الضحايا، كما أبين البيئة التي تنشط فيها الجريمة الإلكترونية لأكشف عن مجتمع حديث يعرف بالمجتمع المعلوماتي مبينا أسباب نشأته وخصائصه وحجمه بالاعتماد على معدلات إحصائية تم رصدها في هذا المجال.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الأول:
مفهوم الجريمة الإلكترونية والفقه الجنائي الإسلامي

المبحث الأول: مفهوم الجريمة في اللغة والاصطلاح

المبحث الثاني: مفهوم الجريمة الالكترونية، خصائصها وأركانها.

المبحث الثالث: مفهوم الفقه الجنائي الإسلامي

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: مفهوم الجريمة في اللغة والاصطلاح

المطلب الأول: التعريف اللغوي للجريمة

يعود أصل كلمة جريمة من جرم بمعنى كسب وقطع، وهي كلمة خصصت قديما للكسب المكروه غير المشروع أو الكسب الآثم، وقد وردت كلمة جرم ويراد منها الحمل على فعل حملا آثما، ومن ذلك قوله تعالى: ﴿وَيَٰقَوْمِ لَا يَجْرِمَنَّكُمْ شِقَاقِيٓ أَن يُصِيبَكُم مِّثْلُ مَآ أَصَابَ قَوْمَ نُوحٍ أَوْ قَوْمَ هُودٍ أَوْ قَوْمَ صَٰلِحٍ ۚ وَمَا قَوْمُ لُوطٍ مِّنكُم بِبَعِيدٍ﴾[1]، أي لا يحملنكم حملا آثما شقاقي ومنازعتكم لي على أن يترل بكم عذاب شديد، مثل ما نزل بمن سبقوكم ممن شاقوا أنبياءهم[2]. والجريمة مفرد، وجمعها جرائم[3].

والجريمة من جرم يجرم جرما، والجرُم هو التعدي، والجُرم الذنب، والجمع إجرام، وجُروم، وهو الجريمة. وقد جرم يجرم وأجرم، فهو مجرم[4].

وأجرم إجرامًا فهو مجرم، يعني: أذنب، والمجرمون في استعمال القرآن أجرموا بالكفر والعناد[5]، قال تعالى: ﴿إِنَّ ٱلْمُجْرِمِينَ فِى عَذَابِ جَهَنَّمَ خَٰلِدُونَ ﴿٧٤﴾ لَا يُفَتَّرُ عَنْهُمْ وَهُمْ فِيهِ مُبْلِسُونَ ﴿٧٥﴾ وَمَا ظَلَمْنَٰهُمْ وَلَٰكِن كَانُوا۟ هُمُ ٱلظَّٰلِمِينَ ﴿٧٦﴾ وَنَادَوْا۟ يَٰمَٰلِكُ لِيَقْضِ عَلَيْنَا رَبُّكَ ۖ قَالَ إِنَّكُم مَّٰكِثُونَ ﴿٧٧﴾ لَقَدْ جِئْنَٰكُم بِٱلْحَقِّ وَلَٰكِنَّ أَكْثَرَكُمْ لِلْحَقِّ كَٰرِهُونَ ﴿٧٨﴾ أَمْ أَبْرَمُوٓا۟ أَمْرًا فَإِنَّا مُبْرِمُونَ ﴿٧٩﴾ أَمْ يَحْسَبُونَ أَنَّا لَا نَسْمَعُ سِرَّهُمْ وَنَجْوَىٰهُم ۚ بَلَىٰ وَرُسُلُنَا لَدَيْهِمْ يَكْتُبُونَ ﴿٨٠﴾﴾[6]، وقال تعالى: ﴿وَلَا يَجْرِمَنَّكُمْ شَنَـَٔانُ قَوْمٍ﴾[7] أي لا يحملنكم أو يكسبنكم بعض قوم على عدم العدل بل المطلوب العدل في جميع الأحوال ومع جميع الناس[8].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والجارم: الجاني، والمجرم: المذنب، وقيل: ولا الجارم الجاني عليهم بمسلم. وفلان أذنب فأجرم، واجترم فهو مجرم، وجريم، ولأهله كسب كأجترم، وعليهم وإليهم جريمة حتى جناية كأجرم[1].

و"الجرم والجريمة والذنب" يقال: جرم، أي: كسب؛ لأن الذي يحوزه فكأنما اقتطعه.. فهو كسب، والكسب اقتطاع[2].

وجرم: جرما، من باب ضر، أذنب، واكتسب الإثم[3].

المطلب الثاني: مفهوم الجريمة في الفقه الجنائي الإسلامي

الفرع الأول: التعريف الاصطلاحي للجريمة

تعرّف الجريمة في الفقه الإسلامي بأنها " محظورات شرعية، زجر الله عنها بحد أو تعزير"[4].

والمحظورات هي إتيان فعل منهي عنه أو ترك فعل مأمور به، وتُوصف المحظورات بالشرعية لأن الشريعة الإسلامية هي التي تُحدد الفعل السَويّ من المنحرف طبقا لمعايير محددة، وهو ما يعني أن الفعل أو الترك لا يعد جريمة إلا إذا نصت الشريعة الإسلامية على ذلك ورتّبت عليه عقوبة، فإذا لم تسن عقوبة على الفعل أو الترك لا يُعد منها جريمة[5]، وهذا المبدأ الشرعي هو الذي استقى منه علماء القانون عن قانونية الظواهر الإجرامية باعتبار أن القانون هو الذي يجرم السلوك[6].

كما عرّف المحدثون الجريمة بأنها: " إتيان فعل محرّم معاقب على فعله، أو ترك فعل محرّم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه "[7].

وهو تعريف يفيد بأن الجريمة هي إتيان فعل مُحرم معاقب على فعله أو ترك فعل واجب معاقب على تركه، حيث قرر الله سبحانه وتعالى عقابا لكل من يخالف أوامره ونواهيه، فإما أن يكون عقابا دنيويا ينفذه الحاكم، وإما أن يكون تكليفا دينيا يكفر به عما ارتكب في جنب الله، وإما أن يكون عقابا أخرويا يتولى تنفيذه الله عز وجل[8].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ويتسم هذا التعريف بشمول كل المعاصي لاعتباره أن الجريمة والإثم والخطيئة ذات معنى واحد؛ فجميعها ينتهي إلى عصيان الله تعالى فيما أمر ونهى، سواء كانت عقوبة العصيان دنيوية أو أخروية. إلا أن جانبا من الفقهاء ينظرون إلى المعاصي من ناحية سلطان القضاء عليها، وما قرره الشارع من عقوبات دنيوية فيخصصون اسم الجرائم بالمعاصي التي لها عقوبة ينفذها القضاء، وفي ذلك قال الماوردي معرفا الجريمة: " أنها محظورات شرعية زجر الله تعالى عنها بحد أوتعزير"[1]. والمقصود بالحد؛ العقوبات المقدرة ويندرج ضمنها القصاص والديات التي قدرها الشارع في موضوعها المنصوص عليها في الكتاب والسنة النبوية، والتعزير هو العقوبات التي يقدرها ولي الأمر بحسب ما يرى به دفع الفساد في الأرض، وسمي تعزيرا لأن به تقوى وتحفظ الجماعة مصداقا لقوله تعالى: ﴿ لَئِنْ أَقَمْتُمُ ٱلصَّلَوٰةَ وَءَاتَيْتُمُ ٱلزَّكَوٰةَ وَءَامَنتُم بِرُسُلِى وَعَزَّرْتُمُوهُمْ وَأَقْرَضْتُمُ ٱللَّهَ قَرْضًا حَسَنًا لَّأُكَفِّرَنَّ عَنكُمْ سَيِّـَٔاتِكُمْ وَلَأُدْخِلَنَّكُمْ جَنَّٰتٍ تَجْرِى مِن تَحْتِهَا ٱلْأَنْهَٰرُ ﴾[2].

وبناء على ذلك فإن المعصية تتلاقى في معناها مع تعريف الجريمة بالمعنى العام لأن المراد من المعصية كل فعل فيه مخالفة لأوامر الله ونواهيه، وكذلك بالنسبة لمعنى الإثم والخطيئة فإنهما يتلاقيان مع معنى الجريمة بالتعريف العام أيضا، وكلها يقوم على معصية الخالق ومخالفة الشرع.[3]

الفرع الثاني: مفهوم الجناية وعلاقتها بالجريمة

يعبر بعض الفقهاء عن الجريمة بلفظ الجناية، ويقتصر البعض على هذا اللفظ في جرائم الحدود[4]، ولإزالة هذا اللبس لابد من تعريف الجناية في اللغة والاصطلاح.

أولا ــ التعريف اللغوي للجناية.

الجناية لغة مصدر جنى يجني جناية، والجناية جمعها جنايات وهي تدل على الذنب والجرم وما يفعله الإنسان مما يوجب عليه العقاب أو القصاص في الدنيا والآخرة[5]، وفي الحديث (لا يجني جان إلا على نفسه)[6]، وقيل الجناية ما يجنيه المرء من خير أو شـــر، جنى فلان ثمرة عمله الصالح إن جنى

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

خيرا، وجنى فلان ثمرة عمله الطالح إن جنى شرا.[1]

وقيل: أن الجناية في الأصل أخذ الثمرة من الشجر فنقلت إلى إحداث الشر، ثم إلى الشر، ثم إلى فعل محرم[2].

ثانيا: التعريف الاصطلاحي للجناية

إن المتأمل في كتب الفقه الإسلامي يجد أن مصطلح الجناية يقتصر على الحدود عند بعضهم، والبعض الآخر يضيف إلى اصطلاح الحدود الجراح وهو ما يؤديه لفظ الجناية من معنى ومقصد عند القائلين به، كما يستعمل لفظ الجناية بكثرة في العديد من الكتب الفقهية من غير أن يرسو على تعريفا محددا يستطيع القارئ من خلاله تصور المسائل والفصول التي هو بصدد قراءتها والبحث من خلالها بالنظر إلى الحد، بل الكثير منهم يكتفي بالتبويب والعنونة بلفظ "كتاب الجناية" ثم يعقبون على إثره في الحاشية بقولهم ويقصد بها الجناية على النفس والبدن.. الخ.

لكن هناك طائفة من العلماء تطرقوا إلى تعريف لفظ الجناية عند بدء كتابهم لبحث مسائل هذا الباب، ومن أشهرهم أصحاب المذهب الحنبلي حيث يقول ابن قدامة: "الجنايات؛ هي كل فعل عدوان على نفس أو مال، لكنها في العرف ـــ لدى الفقهاء ـــ مخصوصة بما يحصل فيه التعدي على الأبدان" [3].

ويقول صاحب الإقناع "الجنايات: جمع جناية، وهي التعدي على الأبدان بما يوجب قصاصا أو غيره"[4].

وقال الفتوحي في منتهى الإرادات "الجنايات: جمع جناية وهي التعدي على البدن بما يوجب قصاصا أو مالا".[5]

كما عرّف علماء الحنفية الجناية بأنها: "اسم لفعل محرم حلّ بمال أو نفس"، وقالوا أيضا: "يراد بإطلاق اسم الجناية الفعل في النفس والأطراف فالأول يسمى قتلا والثاني يسمى قطعا وجرحا".[6]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وعرّفها ابن عرفة المالكي بقوله "فعل هو بحيث يوجب عقوبة فاعله بحد أو قتل أو قطع أو نفي"[1].

وعرّفها العدوي بقوله: "هي إتلاف مكلف غير حربي نفس أو بدن إنسان معصوم أو عضوه أو اتصالا بجسمه أو معنى قائما به عمدا أو خطأ بتحقيق أو تهمة"[2].

ويتضح من خلال هذه التعريفات أن فقهاء الشريعة يقصدون بلفظ الجناية معنيين اثنين؛ الأول معنى عام وهو إطلاق لفظ الجناية على كل فعل محرم شرعا، سواء وقع الفعل على نفس أو مال أو غيرها، والثاني معنى خاص وهو إطلاق لفظ الجناية على الاعتداء الواقع على نفس الإنسان أو أحد أعضائه وهو القتل والجرح والضرب وهو المعنى الذي تعارف عليهم أغلب الفقهاء، والبعض منهم يطلق لفظ الجناية على جرائم الحدود والقصاص[3]، لكن يبقى لفظ الجناية في الفقه الإسلامي على أنه من مرادفات لفظ الجريمة باعتبار أن كل جريمة هي جناية، سواء عوقب عليها بالحبس والغرامة أم بأشد منها.

المطلب الثالث: أركان الجريمة في الفقه الجنائي الإسلامي

كي يعد الفعل جريمة في الفقه الجنائي لابد أن يتوفر على ثلاثة أركان عامة، وهي الركن الشرعي الذي يوجب توفر نص يحظر الجريمة ويعاقب عليها، والركن المادي ويتعلق بإتيان العمل المكون للجريمة سواء كان فعلا أو امتناعا، والركن المعنوي ويتعلق بمدى تكليف الجاني ومسؤوليته عن الجريمة ويعرف أيضا بالركن الأدبي، وهذه الأركان الثلاثة هي عبارة عن قاسم مشترك بين جميع الجرائم غير أن هذا لا يغني من وجود أركان أخرى خاصة بكل جريمة كركن الأخذ خفية في السرقة، وركن الوطء في جريمة الزنا وغيرها وقد بحثها الفقهاء في كتب الفقه الجنائي الخاص حيث تكلموا عن الجرائم بالتفصيل، وسأكتفي بشرح الأركان الثلاثة الأساسية في الفروع التالية:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الأول: الركن الشرعي[1]

توجب الشريعة الإسلامية لاعتبار أي فعل جريمة أن يقابلها نص يحرّم هذا الفعل ويعاقب على إتيانه: وهذا ما يسمى بالركن الشرعي للجريمة.

ويشترط العقاب على الفعل المحرم أن يكون النص الذي حرمه نافذ المفعول وقت اقتراف الفعل، وأن يكون سارياً على المكان الذي اقترف فيه الفعل وعلى الشخص الذي اقترفه، فإذا تخلف شرط من هذه الشروط امتنع العقاب على الفعل المحرم، وعلى هذا الأساس قسم الفقهاء الأحكام الشرعية ـــ أي النصوص ـــ إلى نوعين: أحكام تكليفية، وأحكام وضعية.

أولا ـــ الحكم التكليفي: هو ما اقتضى طلب فعل من المكلَّف، أو كفه عن فعل، أو تخييره بين فعل والكف عنه[2]، ويسمى هذا الحكم تكليفياً لأنه يتضمن إلزام المكلف إتيان فعل، مثل قوله تعالى: ﴿ إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ ﴾[3]، أو إلزام المكلف الكف عن فعل، مثل قوله تعالى: ﴿ وَلَا تَقۡتُلُواْ ٱلنَّفۡسَ ٱلَّتِي حَرَّمَ ٱللَّهُ إِلَّا بِٱلۡحَقِّۗ ﴾[4]، وقوله: ﴿وَلَا تَقۡرَبُواْ ٱلزِّنَىٰٓۖ إِنَّهُۥ كَانَ فَٰحِشَةٗ وَسَآءَ سَبِيلٗا ﴾[5]، أو تخيير المكلف في إتيان الفعل والكف عنه، مثل قوله تعالى: ﴿وَإِذَا حَلَلۡتُمۡ فَٱصۡطَادُواْۚ ﴾[6]، وقوله: ﴿ وَمَن قُتِلَ مَظۡلُومٗا فَقَدۡ جَعَلۡنَا لِوَلِيِّهِۦ سُلۡطَٰنٗا﴾[7].

ثانيا ـــ الحكم الوضعي: هو ما اقتضى جعل شيء سبباً لشيء، أو شرطاً له أو مانعاً منه، وسمي الحكم وضعياً لأنه يقتضي:

1 ـــ وضع أسباب لمسببات، كقوله تعالى:﴿وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقۡطَعُوٓاْ أَيۡدِيَهُمَا﴾[8]، وقوله:﴿ٱلزَّانِيَةُ وَٱلزَّانِي فَٱجۡلِدُواْ كُلَّ وَٰحِدٖ مِّنۡهُمَا مِاْئَةَ جَلۡدَةٖۖ ﴾[9]، فالحكم الأول يقتضي جعل السرقة سبباً في قطع يد السارق، وأما الحكم الثاني فيقتضي جعل الزنا سبباً لجلد الزاني.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ــ أو يقتضي وضع شروط لمشروطات، كقوله تعالى:﴿ لَّوْلَا جَآءُو عَلَيْهِ بِأَرْبَعَةِ شُهَدَآءَ فَإِذْ لَمْ يَأْتُواْ بِٱلشُّهَدَآءِ فَأُوْلَـٰٓئِكَ عِندَ ٱللَّهِ هُمُ ٱلْكَـٰذِبُونَ﴾[1]، وهو حكم يقتضي اشتراط أربعة شهود لإثبات جريمة الزنا، ومثل قول الرسول ﷺ: (لا تقطع اليد إلا في ربع دينار فما فوقه)[2] فهذا الحكم يشترط لقطع يد السارق أن تبلغ قيمة المسروق ربع دينار فأكثر.

3 ــ أو يقتضي عدم الحكم لحضور الموانع، مثل قول الرسول ﷺ : (لا قطع في ثمر معلق)[3]، فهذا الحكم يقتضي أن تعليق الثمر ــ أي عدم حصد المحاصيل والثمار ــ هو مانعاً من القطع في سرقتها، و قوله ﷺ: (لا ميراث لقاتل) [4]، وهو حكم يقتضي جعل القتل الصادر من الوارث مانعاً له من الإرث[5].

فيظهر الفرق بين الحكم التكليفي والحكم الوضعي من وجهين: أولهما أن الحكم التكليفي يقصد به طلب فعل أو الكف عنه أو التخيير بين إتيان الفعل وتركه، أما الحكم الوضعي فالمقصود منه بيان الأسباب والشروط والموانع، وثانيهما أن الحكم التكليفي يكون دائماً في مقدور المكلَّف، فيستطيع أن يفعله أو يتركه إن شاء، أما الحكم الوضعي فقد يكون أمراً في مقدور المكلف وقد لا يكون في مقدوره.

وما يجب التنويه له أن النص الواحد قد يشتمل على حكم تكليفي وحكم وضعي في آن واحد كقوله تعالى:﴿ وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا﴾ [6]، وهو نص يشتمل على حكم تكليفي يتمثل في طلب الكف عن السرقة، و يشمل أيضا حكم وضعي هو جعل السرقة سبباً في قطع يد السارق، كما يجب الإلمام بالحكم الوضعي سواء كان سبباً أو شرطاً أو مانعاً لأنه يبين العقوبة وأسبابها وشروطها وموانعها [7].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني: الركن المادي للجريمة

الركن المادي هو من المبادئ الأساسية المقررة في الفقه الجنائي الإسلامي إذ أنه لا قيام للجريمة بغير ماديات تؤدي إلى نتائج ظاهرة ومحسوسة، وهو يتكون من ثلاثة عناصر أساسية: الفعل، والنتيجة الإجرامية، وعلاقة السببية بينهما، ويظهر الركن المادي في الجريمة عند القيام بالفعل المحظور سواء كانت الجريمة إيجابية أو سلبية*، وقد ينهي الجاني الفعل فتعتبر الجريمة تامة كمن سرق ملك الغير وخرج من محله، وقد يهم الجاني بالسرقة فيضبط قبل الخروج بالمسروقات أو بعد دخوله مباشرة وهو ما يعرف في الاصطلاح القانوني بالشروع في الجريمة، كما قد يرتكب الفعل المحرم من طرف شخص واحد أو بالاشتراك مع جماعة يتفقون على الجريمة فينفذها أحدهم أو بعضهم، أو يحرّض بعضهم بعضا عليها، أو يساعد بعضهم البعض الآخر وهو ما يسمى بالاشتراك في الجريمة.[1]

ولقد استند الفقهاء على ضرورة توفر الركن المادي إلى العديد من الأدلة الشرعية التي من بينها؛ قوله ﷺ: (إن الله تعالى تجاوز لأمتي عما وسوست أو حدثت به أنفسها ما لم تعمل أو تتكلم)[2]، وقال كذلك ﷺ: (إن الله كتب الحسنات والسيئات ثم بين ذلك فمن هم بحسنة فلم يعملها كتبها الله له عنده حسنة كاملة فإن هو هم بها فعملها كتبها الله له عنده عشر حسنات إلى سبع مائة ضعف إلى أضعاف كثيرة، ومن هم بسيئة فلم يعملها كتبها الله له عنده حسنة كاملة فإن هو هم بها فعملها كتبها الله له سيئة واحدة)[3]، وقال في ذلك الإمام الشافعي: الأحكام على الظاهر، والله ولي الغيب لأنه يتولى الثواب والعقاب ولا يعلم الغيب إلا هو جلال ثناؤه، وكلف العباد أن يأخذوا من العباد بالظاهر[4]، واستدل بقوله تعالى ـــ مخاطبا رسوله الكريم ﷺ ـــ في شأن المنافقين:﴿إِذَا جَآءَكَ ٱلْمُنَٰفِقُونَ قَالُوا۟ نَشْهَدُ إِنَّكَ لَرَسُولُ ٱللَّهِ ۘ وَٱللَّهُ يَعْلَمُ إِنَّكَ لَرَسُولُهُۥ ۗ وَٱللَّهُ يَشْهَدُ إِنَّ ٱلْمُنَٰفِقِينَ لَكَٰذِبُونَ ۝١ ٱتَّخَذُوٓا۟ أَيْمَٰنَهُمْ جُنَّةً فَصَدُّوا۟ عَن سَبِيلِ ٱللَّهِ ۚ﴾[5]، وأخذا بهذه الآية الكريمة فقد عامل الرسول ﷺ المنافقين على أنهم مسلمون وأجرى عليهم جميع أحكام الإسلام، لأنهم ظاهرا يبدون الإسلام و لم يعاملهم على أنهم كفار وأنهم

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما قال سبحانه وتعالى: (اتخذوا أيمانهم جنة)، أي يتظاهرون بالإسلام ليتجنبوا أن يطبق عليهم أحكام الكفر.

ولذلك استقر التشريع الإسلامي على أنه لا جريمة ولا مسئولية ما لم تصدر عن المتهم أفعال يعبر بها عن نواياه الإجرامية، وذلك عن طريق حصول الجريمة التامة سواء من حيث الشروع أو الاشتراك والتي تؤدي إلى الإخلال بالأمن الاجتماعي أو الإضرار بالمصالح، ومن المعروف أن إقامة الجريمة باعتبار الماديات يتفق مع الحاجة إلى إقامة الدليل قضاءً على ارتكاب الجريمة حيث يستحيل الإدانة على فكرة حبيسة في النفس[1].

الفرع الثالث: الركن المعنوي للجريمة

يمثل الركن المعنوي الأصول النفسية لماديات الجريمة ومدى السيطرة عليها؛ حيث أن هذه الماديات لا تهم المجتمع إلا إذا صدرت عن إنسان يسأل عنها ويستحق العقوبة المقررة من أجلها، واشتراط صدور هذه الماديات أن تكون لها أصول في نفسية الجاني وأن تكون له عليها سيطرة ممتدة إلى كل أجزائها.

وللركن المعنوي أهمية أساسية في "النظرية العامة للجريمة" فالأصل ألا جريمة بغير ركن معنوي باعتبار أن هذا الركن هو سبيل الشارع إلى تحديد المسؤول عن الجريمة، إذ لا يسأل شخص عن جريمة إلا إذا قامت علاقة بين مادياتها ونفسيته، فهو ركن يضمن العدالة ويحقق أغراض العقوبة الاجتماعية إذ لا يتصور في العدالة أن توقع عقوبة على شخص لم تكن له بماديات الجريمة صلة نفسية فهو ليس في حاجة إلى الردع أو الإصلاح الذي تسعى إليهما.

ولقد استدل الفقهاء بذلك في قوله ﷺ: (رفع القلم عن ثلاث، عن الصبي حتى يبلغ، وعن النائم حتى يستيقظ، وعن المجنون حتى يفيق)[2]، ومؤدى هذا الحديث أن الجريمة لا يحمل تبعتها غير المميز، كما يستخلص من الحديث العلة في انعدام المسؤولية وهي انتفاء التمييز، إضافة إلى ذلك فإن التمييز وحده غير كاف لحمل تبعة الجريمة، فقد يكون الشخص مميزا ولكنه غير حر في سلوكه الذي حصلت به الجريمة كأن يكون مكرها فرغم إدراكه بجرم السلوك إلا أنه لا يستطيع تفادي إتيانه، وبناء

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

على ذلك كانت "حرية الاختيار" شرطا ثانيا لحمل تبعة الجريمة ودليل ذلك قوله تعالى:﴿ إِلَّا مَنْ أُكْرِهَ وَقَلْبُهُۥ مُطْمَئِنٌّۢ بِٱلْإِيمَٰنِ ﴾ [1]، وقوله عز وجل:﴿ فَمَنِ ٱضْطُرَّ غَيْرَ بَاغٍ وَلَا عَادٍ فَلَآ إِثْمَ عَلَيْهِۚ ﴾[2]، وقول الرسولﷺ: (رفع عن أمتي الخطأ والنسيان وما استكرهوا عليه)[3].

وما نستفيده من هذه النصوص أن الركن المعنوي للجريمة مرتبط بشرطي التمييز وحرية الاختيار، وهما شرطان تتحقق بهما وصف الإرادة التي تصدر عنها الماديات الإجرامية ثم تسيطر عليها، فإذا توافر للإرادة هذان الشرطان وصفت بأنها "إرادة معتبرة شرعا" أي صالحة لأن يعتد بها في الأحكام الشرعية، وأن يترتب عليها أثرها[4].

الفرع الرابع: العلاقة بين الركن المعنوي للجريمة والركنين الشرعي والمادي

من غير الممكن فصل العلاقة بين الركن المعنوي والركن الشرعي؛ فلا يؤخذ بالركن المعنوي إلا إذا توافر ابتداء الركن الشرعي لأن الإرادة لا توصف بأنها "إجرامية" إلا إذا اتجهت إلى ماديات أسبغ الشارع عليها صفة غير مشروعة، وبالتالي فإن الركن الشرعي هو مصدر الركن المعنوي إذ التحقق من تجريم الشارع للسلوك سابق على القول بتوافر الركن المعنوي للجريمة.

كما أن الركن المعنوي هو انعكاس لماديات الجريمة في نفسية الجاني ـــ الركن المادي ـــ، فالإرادة تتجه إلى هذه الماديات ولذا فإن تحديد الركن المعنوي لجريمة معينة يفرض تحديد مادياتها لأن الإرادة قد أحاطت بها ثم اتجهت إليها[5].

المطلب الرابع: المفهوم الوضعي للجريمة

عرفت الجريمة في مفهومها الوضعي معان متعددة وذلك حسب وجهات النظر إليها كما يلي:

الفرع الأول: مفهوم الجريمة في القانون

ذهب العديد من علماء القانون إلى تعريف الجريمة بأنها "عمل يجرمه القانون أو امتناع عن عمل يقضي به القانون على أن يكون هذا العمل أو الترك معاقبا عليه"[6]، وعرفت بأنها: "سلوك إرادي غير

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

مشروع يصدر عن شخص مسئول جنائيا، في غير حالات الإباحة، عدوانا على مال أو مصلحة أو حقا محميا بجزاء جنائي"[1].

كما عرفت الجريمة، بأنها " سلوك يُحرمه القانون، ويرد عليه بعقوبة جزائية أو بتدبير احترازي"[2].

ويعرّف القانون الجنائي الجريمة بأنها " إمّا عمل يجرِّمه القانون، أو امتناع عن عمل يقضى به القانون، ولا يعتبر الفعل أو الترك جريمة في نظر القوانين الوضعية إلا إذا كان معاقباً عليه طبقاً للتشريع الجنائي"[3].

ومن أبرز تعريفات علماء القانون للجريمة، ما جاء به الفقيه الإيطالي "كرار ـــ Carrara " الذي يعرف الجريمة بأنها: "خرق لقانون من قوانين الدولة، بفعل خارجي محسوس، صادر عن شخص، لا يبرره قيام بواجب، وممارسة الحق، مىتى تناول القانون هذا الفعل بالعقاب"[4].

وتعريف العالم الأمريكي "جيروم هول" الجريمة بأنها "ضرر محظور بمقتضى القانون الجنائي، مسند على رجل عادي بالغ ارتكبه عن إرادة وقصد، ويجب أن ينال عنه عقابا معيّنا في القانون"[5] .

و الملاحظ من هذه التعريفات وما اطلعت عليه فيما يخص الجريمة في القوانين الوضعية، أن أغلبها يهمل المسائل الأخلاقية ولا يجرمها إلا إذا لحق ضررها المباشر الأفراد أو الأمن أو النظام العام، فعلى سبيل المثال لا يعاقب الزاني إلا إذا أكره أحد الطرفين الآخر، بينما الشريعة الإسلامية تعاقب على الزنا في كل الأحوال لكونها جريمة تمس الأخلاق،كما لا تعاقب أكثر القوانين الوضعية على شرب الخمر ولا تعاقب على السكر لذاته إلا إذا ألحق الأذى بالناس أو المصالح العامة، والعلة في ذلك أن القوانين الوضعية لا تقوم على أساس الدين وإنما تقوم على أساس العرف والتقاليد وهو ما جعلها تختلف من بلد لآخر.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني: مفهوم الجريمة في علم الاجتماع

تطرق علماء الاجتماع للجريمة على أنها كل فعل يتعارض مع ما هو نافع للجماعة وما هو عدل في نظرها، وهو ما تبناه المتخصصون الأنثروبولوجيون في تعريفهم للجريمة نظرا لإمكانية تطبيق هذا التعريف على المجتمعات البدائية التي لا تملك قانوناً مكتوباً، حيث تعرف الجريمة اعتماداً على المفهوم الاجتماعي لها بأنها: انتهاك للعُرف السائد مما يستوجب توقيع الجزاء على من ينتهكه، وأنها ذلك الفعل العدائي والمعارض لتماسك الجماعة التي يعتبرها الفرد جماعته الخاصة[1].

وهو أيضا ما نادى به العالم الإيطالي "جاروفالو" في تحديده لفكرة الجريمة تحديدا لا يرتبط بتشريع معين ولا بزمان محدد، وإنما يصلح لكافة المجتمعات ويسرى على مختلف العصور، بهدف تعميم فكرة الجريمة وتعميم موضوع البحث الإجرامي بدلا من التخصيص الذي يحدده المفهوم القانوني لها نظرا لاختلاف التشريعات باختلاف المجتمعات والأزمنة[2]، حيث خرج بفكرة الجريمة الطبيعية، على أنها الظاهرة التي تعارفت جميع المجتمعات الإنسانية على تجريمها وفرض جزاءات جنائية على مرتكبيها في كل زمان ومكان، وهذا باعتبارها فعل ضار في نظر مختلف المجتمعات وكافة الأزمان، نظرا لتعارضها مع مشاعر الشفقة والأمانة والعدالة المتعارف عليها لدى المجتمعات الإنسانية، وذلك بمنع كل فعل يسبب آلاما جسيمة أو نفسية للغير كجرائم الاعتداء على الأشخاص، ومنع كل اعتداء على ملكية الآخرين كجرائم الاعتداء على الأموال[3].

وبناء على ذلك فإن مفهوم الجريمة في علم الاجتماع يقوم على أساس العوامل ذات الصلة الاجتماعية التي تساهم في وجود الانحراف الإجرامي كالعوامل الأسرية، والاقتصادية والثقافية وعوامل أخرى تتعلق بالبيئة الاجتماعية التي تحيط بالأسرة، ووسائل الإعلام، والعرف السائد وقد نتج عن ذلك مجموعة من المفاهيم المستوحاة من ميولات وأفكار شخصية وهو تباين من شأنه التقليل من أهميتها، كما أن لكل مجتمع مقاييسه الخاصة فما نعتبره نحن جريمة قد لا يكون كذلك عند مجتمع آخر، لكن هذا لا يمنع من وجود العديد من التعريفات التي تعد أكثر أهمية من غيرها.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثالث: مفهوم الجريمة في علم النفس الجنائي

يعتني علم النفس الجنائي بدراسة العوامل النفسية التي تؤدي إلى ارتكاب الجريمة، وذلك من أجل تحديد أوجه الاختلال النفسي التي قد تساهم في إحداث السلوك الإجرامي، وهذا على خلفية أن أسباب الجريمة لا تعود إلى عوامل عضوية فحسب بل قد تكون نفسية أيضا، مما جعل اهتمام هذا العلم ينصب في دراسة تكوين العقلية الإجرامية " الاستعداد أو الميل الذهني لارتكاب الجرائم" لدى المجرم وتتبع كيفية نموها وتطورها، ومدى تأثير العوامل المحيطة به على تكوينه النفسي، ودور هذا التأثير في السلوك الإجرامي، ومن ثم توجه الجهود التي يمكن أن تبذل نحو إصلاحه وتأهيله[1]. وعلى هذا الأساس فإن الجريمة في علم النفس الجنائي تعرف بأنها: "إشباع لغريزة إنسانية بطريق شاذ لا ينتهجه الرجل العادي في إرضاء الغريزة نفسها، وذلك الخلل كمي أو شذوذ كيفي في هذه الغريزة مصحوبا بعلة أو أكثر في الصحة النفسية، وصادفت وقت ارتكاب الجريمة انهيار في الغرائز السامية وعدم الخشية من العقاب"[2].

وهذا يعني أن علماء النفس المهتمون بالسلوك الإجرامي يؤكدون أن الجريمة تُعبر عن موقف يمكن وصفه بأنه تضارب سلوك الفرد مع سلوك الجماعة "ويلاحظ أن الاتجاه النفسي في تفسير الجريمة يعتمد على أن النفس تتكون من مجموعة نوازع تصطدم بمعايير الحياة الاجتماعية وقيود القيم، فتحدّ من جموحها وانطلاقها فيتولد فيها تصادم النوازع، ما يؤدي إلى اختلال في التوازن العام ينتج عنه سلوك إجرامي"[3].

وما يمكن استخلاصه أن مفهوم الجريمة في علم النفس الجنائي لا يتعارض مع المفاهيم الشرعية أو القانونية أو الاجتماعية من حيث إيقاع العقاب ونبذ التصرف الحاصل من طرف الجناة، لكنه يربط الجريمة بالعوامل النفسية المؤثرة في السلوك الإجرامي باعتبارها سبب رئيسي لحصول الجريمة وذلك لاعتبارات عدة من أهمها السعي إلى التخفيف من حدة العقاب الذي يلحق بالجاني والتوجه نحو إصلاحه وتأهيله.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني: مفهوم الجريمة الالكترونية، خصائصها وأركانها

عرفت الجريمة الالكترونية اختلافا كبيرا في الاصطلاحات الدالة على ظاهرة الجرم الناشئ في بيئة التكنولوجيا الحديثة، وهو اختلاف رافق مسيرة تطور ظاهرة الإجرام المرتبطة بتقنية المعلومات ابتداء من اصطلاح إساءة استخدام الكومبيوتر، إلى جريمة الكومبيوتر والانترنت، والجريمة الالكترونية، والجريمة المعلوماتية، وجريمة إساءة استخدام تقنية المعلومات، وجرائم السيبر كرايم Cyber crime ، والجرائم المستحدثة وغيرها.

كما لم يرس تعريف موحد للجريمة الالكترونية نظرا إلى اختلاف وجهات النظر في شأن تعريف المعلوماتية، إلا أن القاسم المشترك بين كل التعريفات هو اعتبار الجريمة الإلكترونية فعل جرمي يقوم على أساس وسائل التكنولوجيا الحديثة.

المطلب الأول: مفهوم الجريمة الإلكترونية في اللوائح والقوانين الوضعية:

تعددت المعايير التي قيلت في تعريف الجريمة الالكترونية ما بين موسع ومضيق لها وفق اعتبارات عدة كاعتبار السلوك الإجرامي من وجهة نظر قانونية، واعتبار المفردات الخاصة بها والمستخدمة في تقنيات الحاسوب وشبكة الانترنت وبيان ذلك في الفروع التالية:

الفرع الأول: مفهوم الجريمة الإلكترونية باعتبار السلوك الإجرامي

تعرّف الجريمة الإلكترونية بأنها "سلوك غير مشروع معاقب عليه قانونا، صادر عن إرادة جرمية ـــ مذنبة ـــ ومحله معطيات الحاسب الآلي"[1]، وهذا السلوك غير مشروع باعتبار أن المشروعية تنفي عن الفعل صفة الجريمة، ومعاقب عليه قانونا لأن إسباغ الصفة الإجرامية لا يتحقق في مجال التشريع الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى ولو كان السلوك مخالفا للأخلاق.

وهو تعريف يبين أن محل جريمة الحاسوب هي المعطيات بدلالتها الواسعة والتي تعني البيانات المدخلة والمخرجة والمخزنة والبرامج على اختلاف أنواعها[2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما عرّفت الجريمة الإلكترونية بأنها " كل أشكال السلوك ـــ غير المشروع ـــ أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي"[1]، وقد اقترحت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في اجتماع عقد لها في باريس عام 1983، تعريفا للجريمة الالكترونية ورد فيه أنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"، إلا أن هذا التعريف انتقد لكونه وسع من نطاق هذا النوع من الجريمة، حيث سوى بين السلوك غير المشروع قانونا والسلوك الذي يستحق اللوم أخلاقيا، وذلك باعتبار أنه ليس بالضرورة أن يكون الانحراف عن الأخلاق والسلوك المؤثم معاقب عليه من قبل المشرع[2].

كما تعرف الجريمة الالكترونية بأنها: " أنماط مستحدثة من السلوك الإجرامي يرتبط بالتقنيات الإلكترونية الحديثة التي صارت محلا لهذه الجريمة أو وسيلة لارتكابها"[3]، وهو تعريف يبين أن الثورة العلمية في مجال الحاسب الآلي والانترنت أدت إلى بروز ظاهرة الإجرام المعلوماتي أو الإجرام الإلكتروني؛ فعن طريق الوسائط الإلكترونية يتم السطو على البنوك، وممارسة جرائم مختلفة كالاتجار في المخدرات والدعارة المنظمة، وتجارة الأسلحة، والسرقة، وتزوير المحررات، والاعتداء على البيانات الشخصية، والنسخ غير المشروع لبرامج الكومبيوتر، وإتلاف السجلات الإلكترونية، وغسيل الأموال باستخدام النقود الالكترونية[4].

ويرى جانب آخر من الفقه الجنائي أن الجرائم الالكترونية هي تلك التي يطلق عليها غش المعلوماتية، ويقصد بها "كل سلوك غير مشروع يتعلق بالمعلوماتية المعالجة ونقلها"[5].

كما تعرف بأنها " الاستخدام غير المصرح به لأنظمة الكومبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكومبيوتر أو ملفات البيانات"[6]، وهو ما جاء به أيضا جانب من

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفقه الجنائي حول تعريف الجريمة الالكترونية بأنها الاستخدام غير المشروع للحواسيب، والتي تتخذ صورة فيروس Virus يهدف إلى تدمير الثروة المعلوماتية، ويتنوع هذا الفيروس حسب الأغراض المتوخاة من زراعته، وذلك كما يلي:

1 ــ اختراق النظام المعلوماتي لأحد البنوك بغرض تحويل مبالغ مالية من حساب العملاء إلى الحساب الخاص للمجرم المعلوماتي.

2 ــ اختراق النظام المعلوماتي للغير لنقل المعلومات المعالجة إليكترونيا أو لنقل برنامج من برامجه كليا أو جزئيا إلى النظام الخاص بالمجرم المعلوماتي.

3 ــ اختراق النظام المعلوماتي للغير بغرض التجسس على المؤسسات الهامة في الدولة أو التجسس على الأسرار الشخصية على الأفراد أو التلاعب في بياناتهم ذات الصفة الشخصية بالحذف أو الإضافة أو التعديل.

4 ــ اختراق النظام المعلوماتي للغير للاستفادة من إمكانات الحاسب الآلي ذاته، وهو ما يطلق عليه ــ سرقة وقت الحاسب ــ .

5 ــ اختراق النظم المعلوماتية لتدمير الثروة المعلوماتية المخزنة فيها كليا أو جزئيا.[1]

الفرع الثاني: مفهوم الجريمة الإلكترونية باعتبار الجانب الموضوعي

وهو مفهوم ينحصر في الجرائم التي تقع على الحاسوب أو في داخل نظامه، حيث تعرّف بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحوّل عن طريقه"[2]. كما عرفت أيضا بأنها"غش Fraud معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها"[3].

كما تعرّف الجريمة الالكترونية بأنها تلك الجرائم التي يكون موضوعها الاحتيال المعلوماتي وجرائم التعرض لحرمة الحياة الخاصة وجرائم التخريب والتعدي على برامج الحاسب الآلي والمعلومات[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وقد أشار جانب من الفقه الوضعي إلى أن الجريمة الإلكترونية تمثل تعديا على أنظمة الكمبيوتر مستهدفة المصالح العامة والمصالح الخاصة التي تهم المجتمع والتي ترتبط باستعمال الحاسوب، ذلك أن العدوان على هذه الأنظمة يمكن أن يهدد الحياة بالشلل، بل قد يصل إلى حد تهديد السلم والأمن الدوليين، خاصة وأن كثيرا من الأسلحة ومنها النووية ترتبط في انطلاقها بأنظمة الكمبيوتر[1].

الفرع الثالث: مفهوم الجريمة الإلكترونية باعتبار الوسيلة أو الهدف

تعرّف الجريمة الإلكترونية بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[2]، وفي هذا الشأن أيضا أجرت منظمة التعاون الاقتصادي والتنمية (OCDE) استبيانا حول الغش المعلوماتي، وجاء في إجابة بلجيكا عن هذا الاستبيان تعريفا للجريمة الالكترونية بأنها "كل فعل أو امتناع من شانه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا، بطريقة مباشرة أو غير مباشرة، عن الاستخدام غير المشروع لتقنية المعلومات"[3].

ويعرف جانب آخر الجريمة الالكترونية بأنها: "الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنت"[4]، لكن يعاب على هذا التعريف عدم إشارته إلى وقوع الجريمة الإلكترونية أيضا على شبكة الانترنت، كما في حال تعطيل الشبكة عن العمل أو إبطاء سرعتها أو إتلاف أنظمتها، ويرى هذا الجانب الفقهي أن من سمات هذه الجريمة أنها جريمة مستترة، وتتسم بالسرعة والتطور في أساليب ارتكابها، وهي أقل عنفا في التنفيذ وعابرة للحدود، ويصعب إثباتها لسهولة إتلاف أدلتها[5].

وعرفت الجريمة الإلكترونية في المادة الأولى من القانون العربي النموذجي الموحد في شأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، بأنها "كل فعل مؤثم يتم ارتكابه عبر أي

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وسيط اليكتروني..." حيث تطبق أحكام هذا القانون بالتحديد على كل جرم يستعمل فيه الوسيط الالكتروني[1] كوسيلة لجريمة ما، وقد يرجع السبب في ذلك إلى رغبة المشرع في تحديد السلوك الإجرامي المستحدث على وجه الدقة، باعتبار أن الأصل في الأفعال هو الإباحة، ولذلك فمن الملائم أن يضبط المشرع نموذج السلوك الذي يعد جريمة حفاظا على حقوق وحريات الأفراد من ناحية، واحتراما لمبدأ المشروعية من ناحية أخرى[2].

وفي هذا الإطار ذهب جانب من الفقه الجنائي الوضعي إلى تعريف الجرائم المعلوماتية، بأنها تلك التي تقع على أموال معنوية لا تغطيها هذه القوانين[3]، وهو تعريف يحصر مفهوم الجريمة الالكترونية في الأموال المعنوية بينما هي تتنوع بتنوع الحق المعتدى عليه، كجرائم العنف والاختلاس والاستيلاء على المال العام، والجريمة المنظمة بصورها سواء تمثلت في الاتجار غير المشروع بالمخدرات أو الاتجار في البشر أو غسيل الأموال، بل وصلت الأمر إلى حد تهديد الأمن القومي للدول.

الفرع الرابع: مفهوم الجريمة الإلكترونية باعتبار ارتباطها بالمعرفة الفنية أو التقنية

وهو جانب لا يهتم بالوسيلة أو موضوع الجريمة الالكترونية فيعرّفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدامات الحاسب الآلي، على أنها "أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[4]، كما عرفت أيضا في هذا الجانب بأنها " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[5]، وعرفت بأنها "الأفعال العمدية التي سببت خسائر

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

للحكومة أو مكاسب للأفراد والمرتبطة بتصميم أو استخدام أو تشغيل النظام الذي تقع هذه الأفعال في نطاقه"[1].

وجاء في تعريف آخر بأنها"جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات"[2].

وعرّفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها "الجرائم التي تلعب فيها البيانات الكومبيوترية للجريمة والبرامج المعلوماتية دورا رئيسيا"[3].

وعلى ضوء ذلك، يتضح عدم وجود تعريفا موحدا متفق عليه في شأن الجريمة الإلكترونية، وكذلك الشأن بالنسبة لمصطلح هذه الجريمة؛ فهناك من يطلق عليها اسم جرائم الحاسب الآلي والانترنت، وهناك من يسميها بالجرائم الإلكترونية، والجريمة المعلوماتية، وجرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات، والجرائم المستحدثة.

وذكر في هذا الخصوص أن الأمم المتحدة قد أشارت في المدونة الصادرة عنها في شأن الجريمة المعلوماتية إلى الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الكومبيوتر أو حتى الجرائم المتعلقة بالكومبيوتر، ولعل ذلك ما يفسر عدم التوصل إلى تعريف موحد لهذه المصطلحات، وإن كان هؤلاء قد اتفقوا ضمنا على وجود ظاهرة تتزايد بمعدلات عالية لتلك الجرائم[4].

وكنتيجة لهذا الاختلاف في تعريف الجريمة الإلكترونية، فإن بعض الدول فضلت عدم تعريف الجرائم الإلكترونية في تشريعاتها تحسبا للتطور العلمي والتقني المستمر ولعدم إمكانية حصر قاعدة التجريم في نطاق أفعال معينة قد تتغير في المستقبل، وهو ما تم ملاحظته على سبيل المثال في المملكة المتحدة حيث انتفى تشريعها الخاص بإساءة استخدام الحاسب الآلي من أي تعريف للجريمة الإلكترونية[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ونفس الموقف حصل لدى المشرع الفرنسي الذي ترك لأهل الاختصاص مهمة تعريف هذه الجريمة، واكتفى في قوانين متعاقبة بتجريم الأفعال المعلوماتية، بعد أن صنفها تبعا لأهدافها كالعبث بالبيانات، والتخريب، والسرقة، والغش، والتحايل[1].

وكنتيجة لما ما سبق، فإنه لاعتبار أي تصرف جريمة إلكترونية يجب أن يتوفر على عنصرين أساسيين هما: العنصر الشخصي ويتعلق بتسخير الفاعل خبرته ومهارته الفنية في ارتكاب الجرم، والعنصر الثاني هو العنصر الموضوعي ويتعلق بمحل ارتكاب الجريمة، حيث يقتضي أن يكون الجهاز الإلكتروني ـــ الحاسوب ـــ " المشغّل" هو المحل لإرتكاب الجرم أو أنظمته، باعتبار أن الجريمة الإلكترونية تستهدف إما المعلومات كسرقتها أو حذفها، وإما الأجهزة كتعطيلها العمدي أو تخريبها بواسطة الفيروسات أو البرامج الهجومية، وقد تستهدف أيضا الأشخاص أو الجهات كالتهديد، والابتزاز أو السرقة ، هذا وقد تستهدف الجريمة الإلكترونية جميع هذه العناصر معا[2].

ويتبين أيضا من خلال التعريفات السابقة، أنها تتحد من حيث موضوع الجريمة في حد ذاتها والوسائط المستعملة بخلاف الجرائم التقليدية، فالجريمة الالكترونية كل أدواتها لها صلة بالتكنولوجيا الحديثة كالحاسوب بجميع معطياته وأنواعه التي من بينها الهواتف الذكية، والألواح الإلكترونية وكل الأجهزة التي تتيح إمكانية الاتصال بشبكة الانترنت وأنظمتها..

كما أضم رأيي إلى تعريف الجريمة الإلكترونية التي جاءت بها المادة الأولى من القانون العربي النموذجي الموحد في شأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، بأنها "كل فعل مؤثم يتم ارتكابه عبر أي وسيط اليكتروني..." نظرا إلى شمولية التعريف حسب رأيي وتوافقه ومبادئ المجتمع الإسلامي باعتبار أن الأصل في الأفعال هو الإباحة، على أن يتم تهذيبه وفق الضوابط الشرعية.

المطلب الثاني: خصائص الجريمة الالكترونية:

نظرا لكون الجرائم الإلكترونية هي من إفرازات تقنية المعلومات فقد أكسبها ذلك طابعا قانونيا خاصا ميزها عن غيرها من الجرائم التقليدية وذلك بمجموعة من الصفات والخصائص، ومن أبرزها ما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

1 ــ لا تتطلب الجرائم الإلكترونية في أغلبها حضور الفاعل في مسرح الجريمة، بل يمكنه تنفيذ جريمته عن بعد سواء من خلال اختراق الشبكة المستهدفة أو اعتراض عملية تحويل مالية، أو سرقة معلومات هامة أو تخريب ونحوها.

2 ــ ومن خصائصها أنها جريمة عابرة للحدود، فاستغلال المجرمين لشبكة الانترنت العالمية جعل من عولمة الجريمة أمرا ممكنا وشائعا حيث أصبح لا يعترف فيها بالحدود الإقليمية للدول، ولا بالمكان ولا بالزمان، وأصبحت ساحتها العالم أجمع الأمر الذي أدى إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم، كما قد يتعذر فيها المطالبة بالتعويض المدني من طرف الضحايا.

3 ــ صعوبة اكتشاف الجريمة الإلكترونية، فالضحية في الغالب لا يشعر بها لكونها مجرد ذبذبات إلكترونية تتحول إلى أوامر تلحق الضرر بالبيانات وفق ما يصبو إليه المجرم المعلوماتي، وكل ذلك يحصل بدون عنف أو اقتحام. (1)

4 ــ هي جريمة لا تترك وراءها أثرا ماديا في مسرح الجريمة بخلاف ما يحصل في الجرائم التقليدية، كما أن مرتكبيها يملكون القدرة على طمس أدلة التقصي في فترة قصيرة وهو ما يجعل الأمور أكثر تعقيدا لدى سلطات الضبط وأجهزة التحقيق(2).

5 ــ كما أنها توصف أيضا بالجرائم الناعمة، لأن الجريمة التقليدية تكاد لا تخلو من استخدام الأدوات الحادة والعنف كجرائم السرقة والسطو المسلح، لكن الجرائم الإلكترونية في الغالب لا يستخدم فيها العنف، ويعود السبب الرئيسي في ذلك إلى عدم مواجهة المجرم بالضحية خاصة وأنها جريمة تتم عن بعد وخلف الأجهزة الإلكترونية.

6 ــ ومن خصائصها أيضا أن أدلة الإدانة في الجرائم الالكترونية هي عبارة عن سجلات الحاسوب أو معلومات رقمية تفيد تورط المجرم وهو ما يثير مشاكل كثيرة أمام القضاء من حيث حجيتها، لذلك فإن البعد الإجرائي للجرائم الالكترونية ينطوي على تحديثات ومشكلات جمة يتطلب

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الأمر فيها الإسراع إلى كشف الأدلة خشية ضياعها، وذلك وفق قواعد التفتيش والضبط الملائمة لهذه الجرائم.[1]

7 ــ كما تحدث الجرائم الإلكترونية خسائر ضخمة وبالغة الخطورة، وهذا راجع إلى الدور الكبير الذي تقوم به تقنية المعلومات في مجال تسيير معظم شؤون الحياة اليومية، إضافة إلى عامل السرية لمعظم الحكومات أمنا ودفاعا وهو ما يظهر فداحة الأضرار الناجمة عن هذه الجرائم كما وكيفا[2].

المطلب الثالث: أركان الجريمة الالكترونية:

الفرع الأول: الركن المادي

يعرّف الركن المادي للجريمة بأنه سلوك إجرامي معين يتطلبه القانون كمناط للعقاب على هذه الجريمة، على أن تتحقق نتيجة ضارة لهذا السلوك الإجرامي كشرط بذاته يتعين قيامه حتى يعاقب على الجريمة، وفضلا عن ذلك يجب أن يرتبط النشاط أو السلوك الإجرامي ونتيجته الضارة بعلاقة سببية، وهو ما يعرف "بالإسناد المادي"[3]، ويقصد بالسلوك الإجرامي الفعل الذي يقترفه الجاني ويبرز في العالم الخارجي مكونا لماديات الجريمة ومسببا لما يترتب عليها من ضرر أو مخاطر، وسواء قصد الجاني من هذا السلوك الإجرامي تحقيق نتيجة معينة أم تحققت النتيجة دون أن تنصرف إرادته إليها[4]، وتعد النتيجة الإجرامية العنصر الثاني من الركن المادي على أن ترتبط بالسلوك الإجرامي بعلاقة سببية، ومدلولها المادي هو الآثار التي تحدثها الجريمة في العالم الخارجي، أما العنصر الثالث في الركن المادي فيتمثل في علاقة السببية، والتي تعني أن السلوك المادي هو الذي أدى إلى تحقيق النتيجة[5].

والسلوك المادي في الجريمة الالكترونية يتطلب توفر بيئة رقمية واتصال بالشبكة المحلية أو العالمية، كما يتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فقد يقوم المجرم بتحضير الحاسب بهدف تحقيق الجريمة كتحميله ببرامج الاختراق على سبيل المثال، أو يقوم بتصميم هذه البرامج بنفسه عن طريق البرمجة، أو يقوم بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة أو أي عمل ممنوع

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ويحمّلها على الجهاز المضيف Hosting Server ، أو يقوم بجريمة إعداد برامج خبيثة تمهيدا لبثها في أجهزة الضحايا.

وكما هو معلوم لا تستلزم كل جريمة اقترانها بأعمال تحضيرية، لذلك يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في الجرائم الالكترونية؛ فشراء برامج اختراق ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال تعد جريمة في حد ذاتها[1].

الفرع الثاني: الركن المعنوي

يقصد بالركن المعنوي العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، بمعنى العلم بعناصر الجريمة وإرادة ارتكابها، ولذلك فإن الركن المعنوي لابد أن يقترن بالقصد الجنائي الذي بدوره ينقسم إلى القصد العام المتمثل في العلم والإرادة، والقصد الخاص المتمثل في نية التملك[2]، فالعلم هو إدراك الأمور على نحو مطابق للواقع، وهو يسبق الإرادة التي يقصد بها الاتجاه لتحقيق السلوك الإجرامي، فالقصد الجنائي العام هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة ولا يمتد لما بعدها، أما القصد الجنائي الخاص فهو ما يتطلب توافره في بعض صور الجرائم بحيث لا يكفي مجرد تحقيق الغرض من الجريمة بل يتعدى إلى نوايا الجاني التي يسعى وراءها بعد تحقق النتيجة.

فعلى سبيل المثال من يقوم بالاستيلاء على البرامج أو البيانات أو المعلومات والنظم المخزنة في ذاكرة الحواسيب أو أي وسائط إلكترونية أخرى، مع علم الجاني بأن هذه الأشياء هي مملوكة للغير ورغم ذلك يقوم بإخراج الشيء من حيازة مالكه وإدخاله في حيازته مصحوبا بنية تملك ما تم الاستيلاء عليه فإن القصد العام والخاص يتوفران في هذه الحالة وبالتالي يتحقق الركن المعنوي[3].

وفي هذا الشأن نجد أن المشرع الأمريكي يتنقل في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخرى يأخذ بالعلم كما في القانون الأمريكي المتعلق بمكافحة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الاستنساخ، ويعود سبب بروز هذه المشكلة إلى ما يعرف بحادثة موريس الذي كان متهما في قضية دخول غير مصرح به على جهاز فيدرالي حيث دافع محامي موريس على انتفاء الركن المعنوي، الأمر الذي جعل المحكمة تقول: "هل يلزم أن يقوم الإدعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به بحيث تثبت نية المتهم في الولوج إلى حاسب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح" ولذلك لجأت المحكمة إلى تبني معيارين هما الإرادة بالدخول غير المصرح به، وكذا معيار العلم بالحظر الوارد على استخدام نظم معلومات فيدرالية دون تصريح[1] .

وبالنسبة للقضاء الفرنسي فإن منطق سوء النية هو الأعم بشأن الجرائم الالكترونية، حيث يشترط المشرع الفرنسي وجود سوء نية في الاعتداء على بريد إلكتروني مثلا خاص بأحد الأشخاص ليتحقق الركن المعنوي[2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث: مفهوم الفقه الجنائي الإسلامي

لمعرفة كل علم يرغب التوصل إليه لابد من تعريفه تعريفا جامعا لمفرداته ومتعلقاته، مانعا، يمنع من دخول غيره فيه، وعلى ضوء ذلك فإن الفقه الجنائي يعرّف باعتبار مفرداته، وباعتبار كونه اسما مصطلحا وفق المطالب التالية:

المطلب الأول: مفهوم الفقه الإسلامي

الفرع الأول: مفهوم الفقه لغة واصطلاحا

أولا ــ تعريف الفقه لغة:

وردت كلمة الفقه في اللغة بمعنى العلم بالشيء والفهم له والفطنة فيه سواء كان الفهم مطلقا[1]، كقوله تعالى: ﴿ وَٱحۡلُلۡ عُقۡدَةٗ مِّن لِّسَانِي ۝ يَفۡقَهُواْ قَوۡلِي ﴾[2]، أو كان الفهم دقيقا[3]، كقوله تعالى: ﴿فَلَوۡلَا نَفَرَ مِن كُلِّ فِرۡقَةٖ مِّنۡهُمۡ طَآئِفَةٞ لِّيَتَفَقَّهُواْ فِي ٱلدِّينِ وَلِيُنذِرُواْ قَوۡمَهُمۡ إِذَا رَجَعُوٓاْ إِلَيۡهِمۡ لَعَلَّهُمۡ يَحۡذَرُونَ ﴾[4]، ومنه قوله عز وجل: ﴿ وَإِن مِّن شَيۡءٍ إِلَّا يُسَبِّحُ بِحَمۡدِهِۦ وَلَٰكِن لَّا تَفۡقَهُونَ تَسۡبِيحَهُمۡۚ﴾[5].

فالفقه بمعناه الخاص هو: الإدراك والفهم الدقيق الذي يتطلب بذلاً لقدر من الجهد العقلي وهو المراد والمقصود من حديث النبي ﷺ: (**من يرد الله به خيراً يفقهه في الدين**)[6]، ولقد غلب لفظ الفقه على علم الدين لشرفه.

ثانيا ــ التعريف الاصطلاحي للفقه:

بعد أن تمايزت العلوم الإسلامية، واستقرت مصطلحاتها وتحددت، أصبح معنى الفقه أخص من معنى الشريعة باعتبار أن أحكام الفقه جزء من أحكام الشريعة، فصار الفقه يُراد به العلم بأحكام العبادات والمعاملات دون باقي الأحكام، أما الشريعة فيشمل معناها إضافة إلى أحكام العبادات والمعاملات أحكام العقائد والأخلاق.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وقد عرَّف علماء الأصول الفقه بأنه: "العلم بالأحكام الشرعية العملية المكتسبة من أدلتها التفصيلية"[1]، وشرح التعريف كما يلي[2]:

العلم: هو مطلق الفهم والإدراك، ويشمل الإدراك اليقيني والظني، لأن من النصوص ما يفيد معناه وحكمه قطعاً، ومنها ما يختلف الفقهاء في تفسيره وتحديد معناه بسبب ما يعتريه من الغموض، فيدل على معناه ظناً.

والأحكام جمع حكم، ويقصد بها ما يُثبت لفعل المكلف من صفة الوجوب أو الحرمة أو الإباحة أو الندب أو الكراهة، ذلك لأن الحكم الشرعي ينقسم إلى هذه الأنواع الخمسة.

أما وصف الأحكام بأنها شرعية، فلأن مصدرها هو الشرع فالعلم بالأحكام الشرعية، هو إدراك أوصاف كافة أفعال المكلفين التي أسبغها الشارع عليها.

أما وصف الأحكام الشرعية وتقييدها بكونها عملية ليخرج من التعريف الأحكام الشرعية التي تتعلق بالعقائد فهي من علم التوحيد، والأخلاق لأنها من علم التصوف، فوصف الأحكام بالعملية معناه الأحكام التي تتعلق بأفعال المكلفين فقط.

ومعنى المكتسب من أدلتها التفصيلية؛ العلم المكتسب من الدليل، وهو العلم الذي تمَّ تحصيله عن طريق النظر والاجتهاد، والمقصود بالدليل التفصيلي هو الدليل الخاص بكل مسألة بعينها على حدة بحيث لا يتناول معها غيرها، فالصلاة مثلاً ورد حكمها الوجوب بدليل خاص تفصيلي في القرآن الكريم في قول الله تعالى: ﴿ وَأَقِيمُواْ ٱلصَّلَوٰةَ وَءَاتُواْ ٱلزَّكَوٰةَ وَٱرۡكَعُواْ مَعَ ٱلرَّٰكِعِينَ ﴾ [3].

وبناء على ذلك فإن موضوع علم الفقه يدور حول معرفة الأحكام الشرعية من وجوب، وحرمة، وندب، وكراهة، وإباحة لأفعال الإنسان التي تصدر عنه في حياته من صلاة، وصيام، وزكاة، وبيع وإجارة، وهبة، أو قتل، أو سرقة، أو جهاد ونحوها.

وهذه الأحكام الفقهية العملية منها ما هو أحكام لمسائل جزئية لا تحصى، ومنها ما هو قواعد شرعية من وضع المشرع نفسه مثل قول النبي ﷺ (**لا ضرر ولا ضرار**) [4]، و(**البينة على المدعي واليمين**

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

على من أنكر) [1]، ومنها ما هو قواعد فقهية من وضع الفقهاء واستنباطهم أخذوها من جزئيات الفقه الإسلامي ومسائله الكثيرة كقاعدة "العبرة في العقود للمقاصد والمعاني لا للألفاظ والمباني"[2]، وقاعدة "من استعجل الشيء قبل أوانه عوقب بحرمانه"[3].

الفرع الثاني: خصائص الفقه الإسلامي

يتميز الفقه الإسلامي عن غيره من التشريعات الوضعية بعدة خصائص وصفات ترفّع بها فوق كل التشريعات، ومن أهم هذه الخصائص ما يلي:

أولاً ـــ الربانية [4].

ويقصد بذلك أن أحكام الشريعة الإسلامية وأنظمتها ليست من وضع البشر الذين يحكمهم القصور والعجز والتأثر بمؤثرات الزمان والمكان، وإنما شارعها صاحب الخلق والأمر في هذا الكون وربُّ كل من فيه، ولهذا يعتبر القرآن والسنة النبوية الشريفة هما المصدران الأساسيان للفقه الإسلامي حيث يتوجب على كل مجتهد أن يتقيد بما ورد في القرآن الكريم وسنة النبي ﷺ في استنباط الأحكام الشرعية، ثم الانتقال إلى يدلان عليه من مصادر تشريعية أخرى، وبما ترشد إليه مقاصد الشريعة العامة وقواعدها الكلية.

وفي ذلك قال الله تعالى: ﴿مَّن يُطِعِ ٱلرَّسُولَ فَقَدۡ أَطَاعَ ٱللَّهَۖ﴾ [5] ، وقال رسول الله ﷺ : **(ألا إني أوتيت القرآن ومثله معه)** [6] أي السنة الشريفة، كما أن السنة شارحة للقرآن، بدليل قول الله تعالى: ﴿وَأَنزَلۡنَآ إِلَيۡكَ ٱلذِّكۡرَ لِتُبَيِّنَ لِلنَّاسِ مَا نُزِّلَ إِلَيۡهِمۡ﴾ [7].

ثانياً ـــ الصبغة الدينية:

يتميز الفقه الإسلامي باعتماده فكرة الحلال والحرام، حيث يستوجب لصحة ظاهرة ما توافر شروط وأركان الظاهرة مع وجوب اتفاق النية ومقاصد الشارع، ولهذا فإن هذه الصفة الدينية للفقه الإسلامي جعلت أحكام المعاملات فيه تتصف بوصفين اثنين:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

1 ــ الحكم الدنيوي؛ ويعرف بالحكم القضائي، وفيه يلتزم القاضي بالحكم بناء على ظاهر الفعل أو التصرف مراعيا في ذلك الأحكام الشرعية، ودليل ذلك قوله ﷺ: (**إنما أنا بشر وإنكم تختصمون إليّ، ولعل بعضكم أن يكون ألحن بحجته من بعض فأقضي له على نحو ما أسمع، فمن قضيت له بحق مسلم، فإنما هي قطعة من النار فليأخذها أو ليتركها**)[1].

2 ــ الحكم الأخروي؛ حيث يبنى الحكم على حقيقة الشيء وواقعه الحقيقي وهو النية والبواعث، وعليه يعتمد المفتي في حكمه.

ثالثاً ــ الشمولية في الأحكام:

كما تتميز أحكام الفقه الإسلامي بشموليتها لكل مناحي الحياة، حيث تتناول علاقات الإنسان بربه، وعلاقته بنفسه، وعلاقته بمجتمعه حيث نجد أحكام العبادات تعمل على تنظيم علاقة الإنسان بربه من صوم وصلاة وحج وزكاة ونذر وأضحية وغير ذلك، وأحكام المعاملات تنظم علاقات الناس بعضهم ببعض سواء كانوا أفراداً أم جماعات حيث تشمل أحكام عقود المعاملات، وأحكام الأحوال الشخصية التي تنظم الأسرة، والأحكام الجنائية التي تعمل على حفظ المقاصد الشرعية، والأحكام الدستورية التي تنظم علاقة الحاكم بالمحكومين وتقرير ما للأفراد من حقوق وما عليهم من واجبات، والأحكام الدولية التي ترعى على سبيل المثال علاقة الدولة الإسلامية بغيرها من الدول في حالتي السلم والحرب والمعاهدات، وأحكام المرافعات التي تُنظم القضاء والدعوى وطرق الإثبات أمام القضاء، والأحكام الاقتصادية والمالية التي تشمل حقوق الأفراد المالية والتزاماتهم، وتنظيم أموال الدولة العامة والخاصة، والأحكام الخُلقية المتعلقة بالصفات والتصرفات المحمودة الواجب التحلي بها، والصفات والتصرفات المذمومة الواجب تجنبها لتحقيق صلات التعاون والتراحم بين الناس[2]، ولقد أفصح القرآن الكريم عن شمولية الشريعة وذخر مبادئها وأنظمتها في قوله تعالى: ﴿مَّا فَرَّطْنَا فِي ٱلْكِتَٰبِ مِن شَىْءٍ﴾[3].

رابعاً ــ المرونة:

تتسم أحكام الفقه الإسلامي في جانب المعاملات بالمرونة والصلاحية الدائمة، لكونها تقوم على المقاصد الأساسية التي تعمل على تحقيق مصالح الناس الثابتة كقاعدة التراضي التي تبنى عليها العقود،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وقواعد ضمان الضرر، وحماية حقوق الإنسانية بقمع الإجرام والجريمة، كما تراعي أحكام الفقه الإسلامي جميع الأعراف والمصالح ووسائل الحياة مهما تغيرت وهو ما عبر عنه العلماء بقاعدة: "تتغير الأحكام بتغير الأزمان" .

خامساً ـــ النزعة الجماعية:

فالفقه الإسلامي يهدف إلى رعاية مصالح الفرد والمجتمع، مع اعتباره للنزعة الجماعية أكثر من الفرد، حيث إذا تعارضت المصلحة الفردية مع الجماعة تُقدم مصلحة الجماعة بشرط رفع الظلم عنه، ومثال ذلك تحريم الاحتكار، ومشروعية التسعير الجبري، والبيع الجبري للمصلحة العامة، كبناء المدارس والمشافي، ومشروعية إقامة الحدود لأخطر الجرائم، ورعاية حقوق الجار[1].

سادساً ـــ قيام الفقه الإسلامي على العقيدة والأخلاق:

تقوم أحكام الفقه الإسلامي على أساس العقيدة التي تكفل لهذه الأحكام التطبيق الذاتي من الأفراد لكونها ترسخ ثقافة مراقبة النفس والخوف من عقاب الخالق، وهو ما يجعل أحكام الفقه أكثر امتثالاً واحتراماً وطاعة. أما الجانب الأخلاقي في الفقه الإسلامي فنجده في أحكام العبادات التي تعمل على تزكية النفس وتطهيرها، كما نجده في أحكام المعاملات التي تقوم على أساس الوفاء بالعقود والعهود والأمانة، واحترام حقوق الآخرين، وتحريم التعدي بكل صوره[2].

سابعاً ـــ التيسير ورفع الحرج:

إن المتتبع لمقاصد التشريع الإسلامي لا يجده قائما على إيقاع الحرج بالناس والتشديد عليهم وإنما يجده قائما على تحقيق مصالح معاشهم وآخرهم بما يتفق مع طاقتهم وحدود فطرتهم، وهي خاصية يمتاز بها الفقه الإسلامي برفع الحرج في التكاليف في الحالات الخاصة حيث أجمع العلماء على أن كل ما يوقع في المشقة والحرج غير المعتاد ليس مشروعاً في الدين، لأن كافة التكاليف والواجبات الشرعية طلب الشارع تنفيذها في حدود الوسع والطاقة، وفي ذلك قال الله تعالى: ﴿ لَا يُكَلِّفُ ٱللَّهُ نَفْسًا إِلَّا وُسْعَهَاۚ ﴾[3]، وقال سبحانه وتعالى: ﴿ يُرِيدُ ٱللَّهُ بِكُمُ ٱلْيُسْرَ وَلَا يُرِيدُ بِكُمُ ٱلْعُسْرَ ﴾[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

فهذه النصوص وغيرها تجزم على أن التشريع الإسلامي لا يكلف الإنسان فوق طاقته، ولا يحمله من المسئوليات فوق إمكانه كي لا يتاح له أي عذر أو حجة في التخلي عن أمر شرعي، أو ارتكاب محظور ديني.

المطلب الثاني: مفهوم الفقه الجنائي الإسلامي ومدلولاته.

الفرع الأول: تعريف الفقه الجنائي اصطلاحا

يعرّف الفقه الجنائي الإسلامي باعتباره اسما مصطلحا؛ أنه جزء من الفقه الإسلامي الشامل وهو يبحث في الجرائم بيانا وثبوتا وشروطا، وفي عقوباتها والقواعد التي تحكمها سواء كانت تلك الجرائم حدودا أو قصاصا أو تعازير[1].

وهو تعريف يبين أقسام الجريمة من حيث العقوبة إلى ثلاثة أنواع هي[2]:

أولا ـــ جرائم الحدود: هي محظورات شرعية زجر الله عنها بعقوبة مقدرة تجب حقا لله تعالى، فتكون العقوبات في هذه الحالة معينة ولا يجوز الإنقاص منها أو الزيادة فيها، كما أنها حق لله لا تقبل الإسقاط ولا يجوز العفو عنها بعد رفع أمرها إلى القضاء، وتتمثل جرائم الحدود في: الزنا، والقذف، وشرب الخمر، والسرقة، والحرابة، والردة، والبغي.

ثانيا ـــ جرائم القصاص والدية: هي جرائم يعاقب عليها بقصاص أو دية ولكل من القصاص والدية عقوبة مقدرة حقا للأفراد فهي أيضا ذات حد واحد وليس لها حد أعلى أو حد أدنى، أما كونها حق للأفراد بمعنى أن للمجني عليه الحق في أن يعفو عنها إذا شاء وهي خمسة أنواع: القتل العمد، والقتل شبه العمد، والقتل الخطأ، والجناية ما دون النفس عمدا، والجناية على ما دون النفس خطأ، ويتولى تنفيذ العقوبة وتوقيعها السلطة المختصة دون غيرها.

ثالثا ـــ جرائم التعزير: هي الجرائم التي يعاقب عليها بعقوبة أو أكثر من العقوبات التعزيرية، ويمثل هذا النوع من العقوبات الجانب المرن من العقوبات التي يراعى عند تقريرها ظروف الزمان والمكان للجريمة والمجرم، كما يراعى فيها الظروف المختلفة للمجتمع بما يحقق المصلحة العامة ويُصلح المجرم ويكف شره، وجرائم التعزير غير محددة كما هو الحال في جرائم الحدود والقصاص والدية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وليس في الإمكان تحديدها، أما أنواعها فتبدأ من الوعظ والتوبيخ لتصل إلى الجلد مرورا بالعقوبات المالية والسجن وقد تصل إلى حد القتل، وهي متروكة للاجتهاد ضمن القواعد العامة للشريعة الإسلامية والمقاصد الكلية للإسلام.

ويعرّف الفقه الجنائي الإسلامي حديثا بأنه: "مجموعة الدراسات التي تتناول التنظيم الشرعي الإسلامي للجريمة كظاهرة اجتماعية، يحددها الشارع ابتغاء مكافحتها. والتنظيم الشرعي الإسلامي للعقوبة وما يساندها من تدابير باعتبارها وسائل المجتمع لمكافحة الجريمة كضرر وخطر اجتماعي"[1].

الفرع الثاني: مدلولات الفقه الجنائي الإسلامي

إن مدلول الفقه الجنائي الإسلامي أو التشريع الجنائي الإسلامي أو نظام العقوبات في الإسلام، هي مرادفات ذات معنى واحد يشمل كل ما تعلق بالجنايات أو الجرائم التي حظرها الشرع الإسلامي واعتبرها مخالفات تترتب عليها عقوبات إما حدية أو تعزيرية[2].

المطلب الثالث: مفهوم العقوبة ومقاصدها في الفقه الجنائي الإسلامي

ترتبط خصائص العقوبة في الشريعة الإسلامية بمفهوم العقاب وأهدافه لكونه تشريعاً إلهياً منزلاً، لذلك فإن خصائصها لن تنفك عن كونها هي الأخرى ضمانات حقوقية وتشريعية تصب في تحقيق مقاصد الشريعة المعتبرة.

الفرع الأول: مفهوم العقوبة في اللغة والاصطلاح

أولا: تعريف العقوبة في اللغة

جاء في لسان العرب أن العقبى جزاء الأمر، وأعقبه أي جازاه، وقيل عقب كل شيء آخره، وقيل العقْب والمعاقب المدرك بالثأر وقيل العقوبة الحبس واعتقبت الرجل أي حبسته[3].

ثانيا: التعريف الاصطلاحي للعقوبة

عرّف الفقهاء العقوبة بتعريفات عدة، أوجزت أهمها كما يلي:

1 ــ عرّفها الحنفية بقولهم: العقوبة تكون على فعل محرم، أو ترك واجب، أو سنة، أو فعل مكروه.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ــ وعرّفها المالكية بأنها: زواجر، إما على حدود مقدرة، وإما تعزيرات غير مقدرة.

3 ــ وعرّفها الشافعية بأنها: جزاء على الإصرار على ذنب حاضر، أو مفسدة ملابسة لا إثم على فاعلها، أو جزاء على ذنب ماض منصرم، أو عن مفسدة منصرمة.

4 ــ وعرّفها الحنابلة فقالوا: العقوبة تكون على فعل محرم، أو ترك.[1]

كما تعرّف العقوبة بأنها: الجزاء المقرر لمصلحة الجماعة على عصيان أمر الشارع.[2]

وتعرّف أيضا بأنها: جزاء وضعه الشارع للردع عن ارتكاب ما نهى عنه وترك ما أمر به.[3]

الفرع الثاني: مقاصد العقوبة في التشريع الإسلامي

تتضح الغايات الأساسية من العقاب في الشريعة الإسلامية كما يلي:

أولا ــ الردع: ويقصد به المنع من الإقدام على ارتكاب الجرائم رهبة من العقوبات المقررة وهو ينقسم إلى ردع عام وردع خاص.

1ــ الردع العام؛ يهدف إلى منع أفراد المجتمع كلهم أو بعضهم من الإقدام على ارتكاب الجرائم اعتبارا بما لحق المجرم فعلا من عقاب نتيجة ما صدر منه من تصرف غير مشروع، وهو مقصد تكلم عنه فقهاء الشريعة كابن الهمام الحنفي، والقرافي المالكي، والماوردي الشافعي، حيث أشاروا فيه صراحة إلى المقصد قائلين بأن الله تعالى وضع العقوبات زواجر لردع ذوي الجهالة حذرا من ألم العقوبة وخيفة من نكال الفضيحة عن ارتكاب ما حظر وترك ما أمر، فهي زواجر شرعت لدرء المفاسد المتوقعة وتحقيق المنع العام.[4]

2 ــ الردع الخاص؛ وينحصر أثره على الجاني الذي نفذّت فيه العقوبة، فبالنظر إلى ما تلقاه من ألم وإيذاء مادي ومعنوي فإن ذلك سيجعله ينتهي عن العودة مرة أخرى إلى العصيان، كما قد يكون الردع الخاص بعقوبة استئصالية تقضي على حياة الجاني لمنع تكرار الجريمة نهائيا نظرا لخطورتها،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والردع الخاص يتحقق هدفه عن طريق جميع العقوبات المقدرة أو المفوضة لأن أثره يقتصر على الجاني فيحد من التفكير في الإقبال على الكثير من الأفعال المجرّمة أو العودة إليها.[1]

ثانيا ــ إزالة أثر الجريمة بما يقابلها من الجزاء:

يعد محو أثر الجريمة من المقاصد الأساسية التي تسعى من وراءها الشريعة الإسلامية وذلك عن طريق فرض العقوبة بجزاء مساو للجريمة حسب جسامتها بهدف إبطال مفعولها وإزالة آثارها، فمن المؤكد أن مقابلة الجريمة بجزاء عادل سيعمل على تهدئة النفوس من اللجوء إلى الانتقام بدافع الثأر والذي سينتج عنه جرائم أشد حدة من الجريمة الأصلية، ودليل ذلك واضح في عقوبة القصاص والديات حيث يقول عز وجل:﴿ وَكَتَبْنَا عَلَيْهِمْ فِيهَآ أَنَّ ٱلنَّفْسَ بِٱلنَّفْسِ وَٱلْعَيْنَ بِٱلْعَيْنِ وَٱلْأَنفَ بِٱلْأَنفِ وَٱلْأُذُنَ بِٱلْأُذُنِ وَٱلسِّنَّ بِٱلسِّنِّ وَٱلْجُرُوحَ قِصَاصٌ ﴾ [2]، فعقوبات القصاص توجب أن يفعل بالجاني مثلما فعل بالمجني عليه مع اشتراط المماثلة عند التنفيذ وهذه أبلغ صور العدل والإنصاف مما يحقق أعلى درجات الرضا لدى الضحية أو وليه وبذلك يتم القضاء على نزعة الثأر والعداوة فتنمحي أثر الجناية وتعود الأمور إلى نصابها[3].

ثالثا ــ إصلاح الجنـــاة: يعد إصلاح الجاني وتقويم سلوكه من الغايات الأساسية للعقوبات الشرعية سواء كان ذلك أثناء تنفيذ العقوبة أو بعدها وهو ما يظهر عمليا في العقوبات التعزيرية؛ فلاشك أن سبب التفويض في اختيار العقوبة وتقديرها إنما المقصد منه الوصول إلى ما هو أصلح وأنسب لحال الجاني، كما أن جواز العفو والشفاعة فيها مع إمكانية التوبة كل ذلك يعمل على إصلاح الجاني وعلاجه، ولذلك نلاحظ أن العقوبات التفويضية تحتل القسم الأكبر في السياسة العقابية بحيث تجتمع مع العقوبات المقدرة أحيانا وفي كثير من الأحيان تقوم مقام العقوبات المقدرة لما يتعذر تحقق بعض شروط إقامتها، كما تنفرد أيضا العقوبات التفويضية بعدد من الجرائم لا حصر له وهو ما يتيح فرص كثيرة لتحقيق إصلاح وعلاج الجناة وإعادة إدماجهم في المجتمع[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الثاني:
أدوات الجريمة الإلكترونية

المبحث الأول: الحاسوب، تعريفه، نشأته وأهميته.

المبحث الثاني: شبكة المعلومات العالمية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: الحاسوب، تعريفه، نشأته وأهميته

كثيرا ما يستعين المجرم التقليدي بأدوات ووسائل مادية متعددة في تنفيذ جرائمه كأدوات تكسير الأبواب، أو نسخ من المفاتيح، بالإضافة إلى أدوات حادة للتعدي على الضحية إذا تطلب الأمر، وهو ما يختلف تماما عن أدوات الجريمة الإلكترونية التي لا تستدعي سوى عدد محدود من الأدوات التقنية أو الفنية ابتداء بالحاسوب وأنواعه*، ويعرف هذا النوع من الأدوات بالعتاد أو الهارد HARD ، والأداة الثانية هي البرامج وتعرف بـــ SOFT ، وأخير النظام الشبكي وهو من الوسائل الأساسية التي يعتمد عليها في الجرائم الإلكترونية لتحقيق المقاصد الجنائية.

المطلب الأول: مفهوم الحاسوب ونشأته

تعددت مسميات هذا الجهاز بسبب غياب المؤسسات التي تعنى بمثل هذه المصطلحات في وقت مبكر من ظهورها وإلى اختلاف اللغات التي تتم الترجمة عنها، حيث استخدم المجمع اللغوي اصطلاح "الحاسب الإلكتروني"، بينما اعتمدت المنظمة العربية للمواصفات والمقاييس اصطلاح "الحاسوب"، بمعنى الآلة الكثيرة الحساب وهو تعريف يتصف بالقصور لأن عمليات الحساب هي فقط من أحد تطبيقاته التي يقوم بها، ولذلك فإنه ليس بالضرورة استخدام مصطلحات عربية إذا كانت غير دقيقة، كما أنه ليس عيبا أن تنفذ كلمات دخيلة إلى اللغة العربية مادامت تؤدي المعنى المرجو من ذلك[1].

الفرع الأول: تعريف الحاسوب لغة

الحاسوب في اللغة من الحاسب وهو عد الشيء وحسب يحسبه، بالضم، حسباً وحساباً: عده، وحسبه حسبة.

وسمي الحساب في المعاملات حساباً، لأنه يعلم به ما فيه كفاية ليس فيه زيادة على المقدار ولا نقصا، ويقال رجل حاسب من قوم حسب وحساب[2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والحاسوب جمع حواسيب وهو اسم آلة من حسَب[1]، وكلمة كمبيوتر Computer كلمة إنجليزية مشتقة من الفعل Compute بمعنى يحسب، وعندما ترجمت إلى اللغة العربية استخدم المؤلفون عدة أسماء وكلمات للدلالة عليها: كالعقل الإلكتروني، والحاسب الآلي، والحاسب الإلكتروني، والحاسوب، والكومبيوتر...الخ.[2] فسمي الحاسوب بهذه الأسماء لما فيه من كفاية في ما يؤخذ منه من المعلومات لدقته فكأنه يحسبها قبل أن يخرجها لنا.

الفرع الثاني: التعريف الاصطلاحي للحاسوب

عرف الحاسوب تعريفات عدة معظمها يتقارب في المعنى، ومن بينها: أنه جهاز إليكتروني يقوم باستقبال البيانات وتخزينها ومن ثم إجراء مجموعة من العمليات المنطقية عليها وفقا لسلسلة من التعليمات (البرامج) المخزنة في ذاكرته، ومن ثم يقوم بإخراج نتائج المعالجة على وحدات الإخراج المختلفة[3].

والحاسوب هو عبارة عن مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة البيانات الداخلة طبقا لبرامج تم وضعها مسبقا للحصول على نتائج معينة[4].

كما يعرف بأنه: عبارة عن آلات صنعها الإنسان لتساعده على إدارة أكبر حجم من المعلومات في أقل زمن ممكن[5].

ويعرّف أيضا الحاسوب بأنه جهاز يتلقى مجموعة من المدخلات في صورة بيانات ليقوم باختزانها واسترجاعها، أو معالجتها وترتيبها ومقارنتها وفقا لأوامر وتعليمات يحتويها برنامج معين بغرض إخراجها كنتائج أو معلومات أو إجابات[6].

والبيانات Data، هي مجموعة من الحقائق الأولية الخام كالأرقام والحروف والرموز والأشكال التي يمكن من خلال استكمالها وترتيبها ومعالجتها الحصول على الإجابات أو المعلومات اللازمة لاتخاذ قرارات معينة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والمعلومات Information، هي بيانات كافية ومرتبة ومصاغة بشكل يجعلها مفيدة في اتخاذ قرارات معينة.

والمعالجة Processing، هي عمليات ينفذها الحاسوب طبقا للبرنامج الموضوع له من قبل المبرمج وذلك وفق لغة خاصة بالحاسوب، ومنها العمليات الحسابية كالجمع والطرح والضرب والقسمة، والعمليات المنطقية كأكبر من، ويساوي، وأصغر من.

والبرنامج Program، هو مجموعة متسلسلة من التعليمات والأوامر يتبعها الحاسوب (حسب اختيار المستخدم) لأداء مهام معينة وفق تعليمات المستخدم. [1]

الفرع الثالث: المراحل التاريخية لنشأة الحاسوب

يعود تاريخ نشأة أول صورة للحاسوب إلى عام 1642م، لما قام العالم الفيزيائي والرياضي الفرنسي باسكال Pascal باختراع أول حاسبة ميكانيكية، وهي عبارة عن مجموعة من التروس تقوم بمعالجة الأرقام وإجراء العمليات الحسابية، بحيث تظهر نتيجة عملية الجمع أو الطرح في أعلى الآلة على هيئة أرقام من صفر إلى تسعة، وهي آلة تشبه في طريقة عملها عداد الكيلومترات في السيارة إلا أن إمكانياتها لا تتعدى إجراء عمليات الجمع أو الطرح فقط، ولقد سميت لغة البرمجة في الحواسيب المعروفة بـــ Pascal باسكال* نسبة لهذا المخترع[2].

ولقد مرت نماذج الحاسوب بمراحل عديدة حيث شهدت في كل مرة تحسين في الأداء والنموذج وذلك إلى غاية سنة 1944م، أين تم تصميم أول حاسبة آلية رقمية (Mark I) بواسطة فريق من الباحثين من جامعة هارفارد، وبمساعدة مهندسين من شركة IBM* .

و بين عامي 1943 و 1946م قام المهندسان برسبير ايكرت (Presper Eckert) وجون ماشلي (John Mauchly) باختراع أول حاسب آلي رقمي عملاق (ENIA C) يتكون من 18000 صمام مفرغ، ويتطلب ضبطا يدويا للتحكم في البرامج التي يعمل بها، كونه لا يستطيع تخزين التعليمات وهو أسرع من (Mark I) بمئات المرات، وكان يزن 30 طنا ويحتل مساحة 500م^2، وفي عام 1951م،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

واصل هذان المهندسان أبحاثهما حيث تمكنا من اختراع أول حاسب يقوم باختزان البرنامج ويعمل على هذا المبدأ وسمي بـــ (EDVAC)، وبعد هذه الفترة شهد إنتاج الحواسيب أجيال عديدة إلى أن وصلت إلى ما عليه حاليا وبيانها كما يلي[1]:

الجيل الأول: 1951 ــ 1957 م:

من أبرز ملامح هذا الجيل:

ــ ظهور الحاسب الآلي بشكل تجاري في 14 جوان 1951م حيث اشترت مصلحة الإحصاءات الأمريكية أول جهاز من نوع Univac لاستخدامه في جدولة الإحصاءات السكانية.

ــ استخدام الصمامات الإلكترونية المفرغة وأنابيب أشعة المهبط بطاقة تخزينية تصل إلى 2000 كلمة.

ــ استخدام لغة الآلة* (Machine Language) حيث تكتب التعليمات للحاسب على شكل سلسلة من الأرقام.

ــ كما كان التركيز في هذه الحواسيب على القدرة الحسابية لا غير.

ــ واستخدم الشريط الممغنط عام 1957م كوحدة تخزينية سريعة وذات طاقة عالية مع قارئ البطاقات المثقبة كوحدة إدخال المعلومات للحاسب الآلي.

الجيل الثاني: 1957 ــ 1965م :

وتميز هذا الجيل بما يلي:

ــ استخدام ما يسمى بالترانزستور* بدلا من الصمامات المفرغة وقد فتح هذا الاختراع آفاقا جديدة في الالكترونيات عموما وفي مجال الحاسوب خصوصا. حيث يتميز الترانزستور مقارنة بالصمامات المفرغة بصغر حجمه، وعدم استهلاكه للطاقة إضافة إلى سرعته العالية في التنفيذ.

ــ كما أصبحت البرمجة أقل تعقيدا بعد ظهور لغة التجميع (Assembly Language) التي تستخدم مختصرات للحروف بدلا من الأرقام مثل (Sub) وتعني (Subtract) أطرح.. وهكذا.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ و ظهرت ذاكرة الأقراص الممغنطة بصفتها وسيلة تخزين ذات قدرة تخزينية عالية حيث يمكن الوصول للبيانات المخزنة عليها بسرعة.

ـــ كما ساهم اختراع الترانزستور في ظهور الحواسيب الأقل حجما من سابقيها.

ـــ وتم في هذه المرحلة استخدام حزم البرمجيات الجاهزة وأنظمة التحكم في الإدخال والإخراج ومترجم البرنامج (Compiler) .

ـــ كما اقتصر استخدام الحاسب الآلي على الجامعات والمنظمات الحكومية والهيئات التجارية، و لم يكن شائع الاستخدام لدى عامة الناس.

الجيل الثالث: 1965 ـــ 1972م:

من أبرز ملامح هذا الجيل:

ـــ ظهور الدوائر الكهربائية المتكاملة (Integrated Circuit) وهي عبارة عن دوائر إلكترونية متكاملة على شريحة صغيرة من السليكون لا يتجاوز حجمها 1سم^2، وتحتوي على ملايين من المعدات الإلكترونية.

ـــ تميز هذا الجيل بسرعة أكثر وقدرة تخزينية أكبر من سابقيه.

ـــ ظهرت الحواسيب الآلية ذات الحجم المتوسط.

ـــ ظهر نظام المشاركة في الوقت (Time Sharing) وهي عملية تنظيم الحاسب الآلي المختلفة من عمليات إدخال، ومعالجة الوصول إلى الاستخدام الأمثل لوحدة المعالجة المركزية، ما ساعد على سرعة استجابة الحاسب.

ـــ كما ظهرت شبكات الحاسوب (Computer Network) مما أتاح إمكانية الاتصال بالحاسب الرئيسي عن طريق نهاية طرفية من مكان بعيد.

الجيل الرابع: 1972 ـــ 1980م:

وتميز هذا الجيل بما يلي:

ـــ ظهور الدوائر الكهربائية المتكاملة الكبيرة، وهي عبارة عن دوائر تحوي ملايين الترانزستورات موضوعة على شريحة من السليكون.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ ظهور أول معالج دقيق* (Micro Processor).

ـــ و أصبح بالإمكان استخدام هذا المعالج في صناعات أخرى كالساعات الرقمية، والسيارات، وحاسبات الجيب، والأجهزة المترلية والحاسبات الشخصية...

ـــ ظهور لغات جديدة للبرمجة، وقواعد البيانات والشرائح الممتدة.

ـــ تطور وسائل اتصالات البيانات.

ـــ تطور وسائل تخزين البيانات كأقراص الليزر، والأقراص الممغنطة والأشرطة الممغنطة التي تصل سعة بعضها آنذاك إلى (Giga Byte)* .

الجيل الخامس: 1980 ـــ حتى وقتنا الحاضر:

سمي الحاسوب بداية من الجيل الخامس بـــالحاسوب الشخصي أو ما يعرف بالـــ PC لأنه في بداية هذه المرحلة فقط استطاع الأفراد الحصول بصفة عامة على الحواسيب واستعمالها في الأغراض الشخصية ومنذ تلك الفترة بدأت الحواسيب تشهد باستمرار تطورا مذهلا فاق كل التوقعات حتى أصبح من الضرورات الحيوية للإنسانية جمعاء[1].

الفرع الرابع: أهمية الحاسوب

تكمن أهمية الحاسوب في تبسيطه لكثيرٍ من الأعمال الصعبة أو التي تحتاج وقتاً طويلاً لإتمامها؛ كالأعمال الصّناعيّة، والتّجارية، والإدارات الحكوميّة، والجامعات والمعاهد، ويعتبر الحاسوب وسيلةً ذات قدرة عالية على حل المسائل الرّقميّة، بالإضافة إلى دقّته في حفظ واسترجاع المعلومات، وتصميم الوثائق والصور وإظهارها.

ولقد أصبحت الحواسيب توفر لنا منظومة مجمعة من المعلومات والخدمة التعليمية، والتسويق والاتصالات المباشرة، وخدمات البريد الإلكتروني، وخدمات الفواتير والحسابات واستحداث التطبيقات، وإدارة قواعد بيانات المعلومات، وتوفير البرمجيات بسرعة فائقة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

و ساهم الحاسوب أيضا في تنسيق أعمال الشركات الكبرى، كالإحصاءات المالية الدورية والجداول الالكترونية، وتصنيف البيانات، وتلخيص المعلومات، والخدمات التجارية للبريد الإلكتروني، وطباعة الفواتير وإرسال الشيكات والدفع الالكتروني، وتبادل الآراء والمعلومات بين عشرات الألوف من الشركات والمنشآت المالية والتجارية، كما سمح ذلك بتنفيذ نوعيات خاصة من الصفقات التعاقدية بطريقة آلية.

أما في مجال التجارة والأعمال فقد ساهم الحاسوب في توسيع نطاق السوق الإلكترونية وأصبحت السلع المعروضة للبيع متاحة على المستوى العالمي وفق أسواق افتراضية، ويقوم الحاسب الآلي بتنظيم عمليات التوثيق والتعاقد ومعالجة كل الأمور المتعلقة بنشاط السوق على المستوى العالمي.

أما في مجال التعليم فالكثير من مؤسسات التعليم بدول العالم تعتمد على تقنية المعلومات ـــ بقدر متفاوت ـــ من أجل تسهيل المناهج المختلفة، كما أصبح للحاسوب أهمية بالغة في مجال الطب لما حققه من نجاحات باهرة في هذا المجال، ولو قمنا بتعداد أهمية الحاسوب في وقتنا الحاضر لتطلب أطروحة منفصلة لا نعلم مدى حجمها، ولذلك يمكن القول بأن أهمية الحاسوب في عصرنا الحالي لا تعد ولا تحصى خاصة وأنه أصبح من الضرورات الحيوية في حياة الناس[1].

المطلب الثاني: دور الحاسوب في الجريمة الإلكترونية

للحاسوب أدوار مختلفة في مجال الجرائم الإلكترونية، فقد يكون وسيلة للإجرام الإلكتروني وقد يكون ضحية للجريمة، كما يمكن أيضا أن يلعب دور أساسيا في اكتشاف الجريمة الإلكترونية، وبيان ذلك كما يلي:

أولا: الحاسوب أداة للجريمة

يعد الحاسوب من الأدوات الأساسية المستعملة في تنفيذ العديد من الجرائم الإلكترونية، كسرقة الأموال وذلك عن طريق إرسال أوامر تنفيذ السرقة بواسطته، كما يستخدم في جرائم التزوير والاستيلاء على الأرقام السرية للبطاقات الإلكترونية، ويستعمل أيضا في اختراق قواعد البيانات الخاصة بهيئات مختلفة تتسم بالسرية التامة، كأن يقوم المجرمون بتخريب المعلومات أو التلاعب بها أو

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

تحويرها أو نشرها للعامة أو الابتزاز بها، كما يستخدم أيضا كوسيلة في تنفيذ أعمال إجرامية فائقة الخطورة كالتحكم في مسارات الطائرات والسفن، أو التنصت الجوسسي وغيره[1].

ثانيا: الحاسوب بيئة للجريمة الالكترونية

في كثير من الحالات يستغل مجرمو المعلوماتية الكومبيوتر لاستخدامه كبيئة لجرائمهم حيث يخزنون فيه برامج القرصنة والفيروسات أو ينتجونها بواسطته ومن ثم يهاجمون بها، كما يستخدمونه كبيئة لإنتاج ونشر المواد غير المشروعة وإجراء صفقات المخدرات والقمار ونشر الرذيلة ونحوها[2].

ثالثا: الحاسوب هدفا للجريمة

لقد ثبت أن أغلب الجرائم الإلكترونية تستهدف الحواسيب لأغراض عدة من بينها؛ الاختراقات التي يتعرض لها الحاسوب من أجل الوصول إلى نظمه، أو زراعة الفيروسات لتدمير معطياته، أو سرقة ملفاته أو تغييرها، أو المساس بالمعلومات المخزنة به خاصة منها ذات السرية العالية كملفات الحالات الجنائية أو المعلومات العسكرية وخطط التسويق والتصنيع، أو سرقة الأسرار التجارية ونسخ المصنفات المحمية كالبرامج ونقلها غير المصرح به ، أو تعطيل كفاءة أنظمته وغيرها من الجرائم التي تستهدفه حيث يكاد الحاسوب أن يكون العنصر الأساسي الأول المستهدف في الجرائم الإلكترونية.

رابعا: الحاسوب مستكشف للجريمة الإلكترونية

وبالرغم من المساوئ التي تصدر من الحاسوب في الحالات التي يستعمل فيها كأداة للجرائم الإلكترونية، فإنه في نفس المجال ـــ مجال الجرائم الإلكترونية ـــ يساهم بدور فعال في مساعدة المحققين الجنائيين لكشف الجرائم المستحدثة وتتبع فاعليها، كما يساهم الحاسوب بشكل واسع في إبطال أثر الهجمات التخريبية لمخترقي النظم، وتقصي الفيروسات وقراصنة البرمجيات والتصدي لهم.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثالث: برامج الحاسوب (Computer Programs Software)

الفرع الأول: تعريف برامج الحاسوب

تعرف برامج الحاسوب بأنها مجموعة متسلسلة من التعليمات أو الأوامر يتبعها الحاسوب (حسب رغبة واختيار مستخدم الجهاز) للقيام بعمليات مختلفة، كالعمليات الحسابية، أو المقارنة المنطقية[1].

والبرمجيات هو اصطلاح يطلق على جميع البرامج اللازمة لتشغيل الحاسوب وتنظيم عمل وحداته المختلفة. وهو تعريف يشمل نظم التشغيل (Operating System) ، وكذلك البرمجيات المعيارية (Standard Software) التي يقوم مصنعو الحاسوب (Computer Manufactures) بإعدادها حيث تمكن المستفيدين من استغلال عمل الحاسوب على أفضل وجه، وكذلك يشمل هذا التعريف البرامج التطبيقية (Applications Programs) التي تلزم لاستخدام الحاسوب[2].

الفرع الثاني: أنواع برامج الحاسوب

تنقسم برامج الحاسوب إلى نوعين رئيسيين هما: برامج النظام والتي تعرف أيضا بالبرامج المقيمة (Resident Programs or Systems Programs)، والبرامج التطبيقية (Applications Programs) وبيانها كما يلي:

أولا: برامج النظام Systems Programs

برامج النظام عبارة عن مجموعة من البرمجيات الجاهزة التي تكمن وظيفتها في ضبط وإدارة التحكم بكافة الوحدات الأساسية المكونة للحاسوب وفق ما تحتويه هذه الوحدات من معلومات وبيانات، فهي برامج تتحكم في الوظائف الأساسية لنظام الحاسوب وفي الغالب يتم تثبيتها من طرف الجهة المصنعة للحواسيب ومن أنواعها ما يلي[3]:

1 ـــ أنظمة التشغيل Operating Systems :

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

يقصد بها البرامج التي تقوم بالتحكم والتنسيق بين الأجزاء المادية والبرمجية للحاسوب، كالتحكم في مسار البيانات، ووحدة المعالجة المركزية، ووحدة الذاكرة الرئيسية وأجهزة الإدخال والإخراج الملحقة بالحاسوب وتنسيق العمل بينها جميعا، وذلك لجعلها تستجيب لأوامر المستخدم، ومن أهم نظم التشغيل نظام الدوس* (DOS) الشهير، وهو نظام أساسي في تشغيل الحواسيب حيث يقوم بإدارة جميع العمليات التي يرغب المستخدم في أدائها عن طريق الحاسوب، كما يتحكم هذا النظام في تشغيل البرامج واستخدام وحدات الحاسوب والأجهزة الملحقة المتصلة به، ونظرا لصعوبة التعامل مع هذا النظام لدى عامة المستخدمين حيث يتطلب الكفاءة في الإعلام الآلي كونه يتعامل مع المستخدم عن طريق كتابة أوامر المستخدم عن طريق لوح المفاتيح كي يستجيب الحاسوب، ولذلك طور نظام تشغيل جديد والمعروف بنظام النوافذ WINDOWS وهو نظام سمح لعامة المستخدمين التعامل مع الحاسوب بسلاسة تامة كونه يستجيب لأوامر المستخدم عن طريق الفأرة دون الحاجة إلى كتابة الأوامر، وقد عرف هذا الأخير تطورا مستمرا فاق كل التوقعات حيث أصبح بالإمكان التعامل مع الحاسوب عن طريق الصوت أو النظر دون الحاجة إلى الكتابة أو استعمال الفأرة أو لوح المفاتيح..

2 ــ مترجم اللغة Language Translator :

هو برنامج نظامي يعمل على ترجمة البرامج المكتوبة بلغات الحاسب المختلفة التي يستخدمها المبرمجون والمستخدمون للحواسيب إلى لغة الآلة Machine Code حيث تتحول إلى ذبذبات كهرومغناطيسية تسمح للحاسوب التعامل معها، ثم يقوم البرنامج بعملية عكسية يحول فيها لغة الحاسوب إلى لغة المستخدم فتظهر على الشاشة بلغة البشر.

3 ــ نظام إدارة قواعد البيانات Database Management System :

وهو عبارة عن مجموعة من البرامج التي تتيح استخدام البيانات المخزنة والمعروفة بقاعدة البيانات وذلك من خلال البرامج التطبيقية.

4 ــ البرامج المساعدة Utility Programs :

هي عبارة عن مجموعة من البرامج التي تقوم بالعديد من العمليات التي يتكرر استخدامها كنسخ الملفات أو دمجها أو فرز وترتيب البيانات وغيرها من العمليات والمهام المختلفة.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثانيا: البرامج التطبيقية Applications Programs

هي برامج عادة ما تكون جاهزة تنتجها شركات تجارية عالمية، وتختلف مهامها من برنامج لآخر حسب متطلبات مستخدمي الحواسيب، ومن أهمها ما يلي:

1 ــ البرامج التطبيقية الجاهزة Applications Packages :

وهي البرامج الأكثر انتشارا واستعمالا لدى مستخدمي الحواسيب، أما أنواعها فتغطي معظم المجالات التي لها علاقة باحتياجات المستخدمين، ومن أكثر هذه البرامج شيوعا ما يلي:

1 ــ 1 ــ برامج معالجة الكلمات Word Processing : هي برامج متخصصة في كتابة وتحرير النصوص والوثائق، حيث تتيح عدة اختيارات في مجال تحرير النصوص كإدخال التعديلات عليها، أو استرجاعها أو طباعتها وغير ذلك، ومن أشهرها برنامج الورد Word الذي أنتجته شركة مايكروسوفت الدولية.

1 ــ 2 ــ برامج الجداول Spread Sheets : تتيح هذه البرامج إمكانية تنظيم البيانات والأرقام في جداول من صفوف وأعمدة، كما تتيح إمكانية الربط بين هذه البيانات وإعداد الإحصائيات والرسوم البيانية المتعلقة بها، إضافة إلى إمكانية إجراءها للعديد من العمليات الحسابية والمنطقية..، ومن أنواعها على سبيل المثال، برنامج الإكسل Excel، وبرنامج الأكسيس Access وبرنامج Quatro.

1 ــ 3 ــ برامج قواعد البيانات Database Programs : هي برامج تتيح إمكانية إنشاء الملفات وتجميعها كقواعد للبيانات حسب علاقات معينة تربط بينها وهو ما يتطلبه إنشاء موقع إلكتروني مثلا، ومن بين هذه البرامج، DBASE IV، PARADOX، ORACLE .

1 ــ 4 ــ برامج النشر المكتبي Desktop Publishing : تسمح هذه البرامج بإعداد وترتيب النصوص مع إدماج الصور والرسوم بها وإعدادها ومن ثم توجيهها للطباعة، وهي تستخدم بكثرة في المجال الصحفي كتصميم الجرائد والمجلات، ومن أمثلتها: Page Maker، Corel Draw، Microsoft Publishing.

هذا بالإضافة إلى العديد من البرامج المتخصصة التي تظهر باستمرار وفق متطلبات مستخدمي

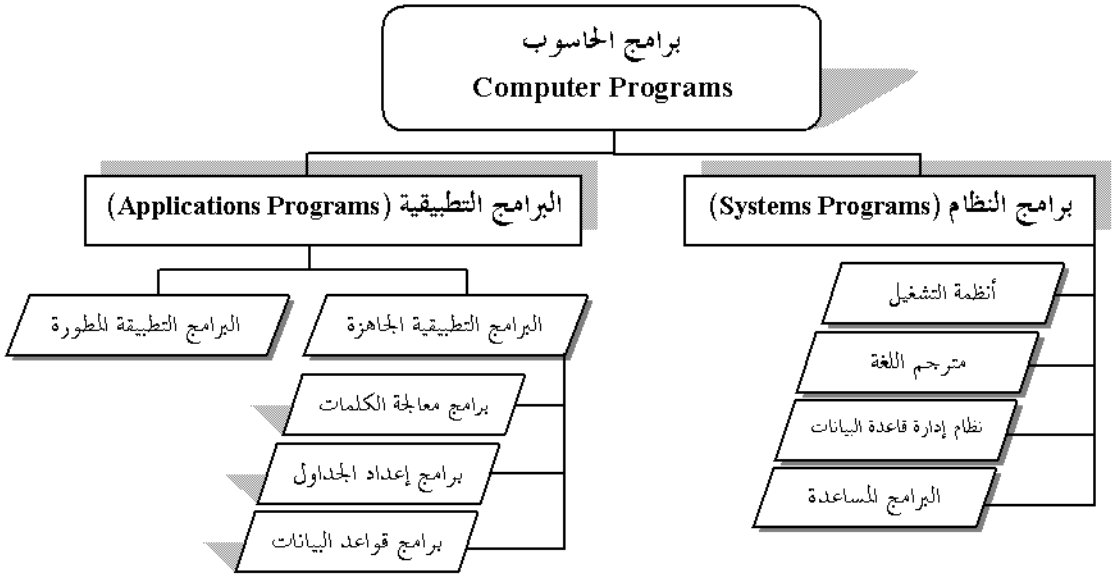
(1) الإحالات في النسخة المطبوعة.
الحواسيب في مجالات متعددة.
(2) الإحالات في النسخة المطبوعة.

.../.....

2 ــ البرامج التطبيقية المطورة Custom Programs:

وهي نوع من البرامج التطبيقية الخاصة التي يتم تصميمها وفق الطلب لتناسب احتياجات وأنشطة المستفيد التطبيقية ولذلك فهي غير معممة، كما تختلف من حيث الأداء حسب نشاط كل مستفيد، ومن أمثلتها برامج التسيير المالي للمؤسسات، برامج الفوترة، برامج تسيير المخزونات وغيرها.

والشكل التالي يوضح أنواع البرمجيات وعلاقاتها:



شكل رقم (01) يوضح أنواع البرمجيات وعلاقاتها

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

المبحث الثاني: شبكة المعلومات العالمية INTERNET

الانترنت هي أبرز ثمرة أنتجتها تلاحم ثلاث ثورات تقنية؛ ثورة المعلومات، وثورة الاتصالات، وثورة الحواسيب، كما تعتبر من أبرز النماذج العالمية استفادة من خدمات الشبكة الرقمية المتكاملة(Integrated Digital Network).

وتعد الانترنت إحدى أكبر موارد المعلومات في هذا العصر، كما تمثل أكبر شبكة معلومات في العالم وثاني أكبر شبكة اتصالات في العالم بعد شبكة الهاتف، حيث تربط مئات الآلاف من الشبكات المحلية، والملايين من أجهزة الحواسيب ومئات الملايين من المستخدمين الذين ينتشرون في أكثر من مائتي دولة، ويعود أهم أسباب نجاح الشبكة وانتشارها هو اعتمادها للغة واحدة في الاتصال مع جميع الأجهزة المرتبطة بها على المستوى العالمي وهو ما يعرف بنظام أو بروتوكول الاتصال المشهور بـــ (TCP/IP)، ومن مقومات نجاحها ما تميزت به من خصائص لا تعد ولا تحصى وأبرزها أنها وسط ثنائي الاتجاه لتبادل المعلومات، بمعنى أن مستخدم الانترنت له القدرة في تلقي أو بث ما يريد نشره[1].

المطلب الأول: مفهوم شبكة الانترنت لغة واصطلاحا

الفرع الأول: تعريف شبكة الانترنت في اللغة

الشبكة لغة: جمع شبكات، وشباك، وشبَكَ. والشبكة شرَك الصياد في البر والبحر، وأكثر ما تتخذ من الخيط المشبّك، والشبكة كل متداخل متشابك[2].

أما التعريف اللغوي للفظ الانترنت فلم أعثر عليه في القواميس اللغوية التي اطلعت عليها وقد يعود سبب ذلك إلى حداثته[3] واختلاف مسمياته، أما أصل لفظ الانترنت هو ترجمة حرفية لكلمة انجليزية INTERNET، وهي مركبة من مقطعين INTER اختصارا لمصطلح "International" بمعنى

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

دولي، وNET اختصارا لكلمة "Network" التي تعني الشبكة، ومجموع الكلمتين هو: International Network بمعنى الشبكة الدولية[1].

ولقد عرفت الانترنت مسميات مختلفة بسبب اختلاف وجهات النظر إلى هذا النوع من التكنولوجيا الحديثة، ومن بين هذه الأسماء؛ "الشبكة العالمية"، " شبكة الشبكات"، "الشبكة العنكبوتية"، "الطريق السريع الرقمي"، "كود النقل المتزامن".. لكن ما يمكن تسجيله في الوقت الحاضر هو تعميم لفظ الانترنت في أغلب المجالات على جميع المسميات الأخرى.

الفرع الثاني: التعريف الاصطلاحي للانترنت

لم يرس مصطلح الانترنت على تعريف كامل وشامل، الأمر الذي دعا إلى محاولة الجهات التقنية والقضائية إلى وضع تعريفات لها والتي اتسمت بالطابع الموضعي للشبكة وذلك كما يلي.

أولاـــ المفهوم التقني للانترنت: جاء هذا الاتجاه بتعريفات عدة للانترنت من بينها:

الانترنت هي: نظام المعلومات العالمي الذي يرتبط منطقيًا بمساحة عنونة متميزة عالميًا بناءً على بروتوكول الانترنت (IP) أو امتداداته؛ ويمكنه دعم الاتصالات باستخدام مجموعة بروتوكول مراقبة الإرسال (TCP/IP) أو امتداداتها، أو البروتوكولات المتوائمة مع IP الأخرى؛ ويوفر أو يستخدم خدمات رفيعة المستوى منسقة على الاتصالات والبنية الأساسية ذات الصلة الموضحة في هذه الوثيقة، أو يُتيح الوصول إليها، بشكل عام أو خاص[2].

وتعرّف أيضا بأنها شبكة تتيح للشبكات المعلوماتية المختلفة أن تنضم إليها عن طريق استخدام بروتوكول TCP/IP، والبريد الإلكتروني e-mail، ومجموعات الأخبار News Groups، وبروتوكول نقل الملفات FTP (File Transfer Protocol)، وبنوك المعلومات Data Banks [3].

كما تعرّف بأنها: اختصار لعبارة International Network وتعني الشبكة العالمية وهي عبارة عن مجموعة لا متناهية من أجهزة الحواسيب حول العالم تتبادل المعلومات فيما بينها عبر خطوط الهاتف[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وجاء في تعريف آخر بأنها: شبكة عالمية من الحواسيب التي تعتمد في ارتباطها على بروتوكول TCP/IP، والبروتوكولات الأخرى للاتصالات فائقة السرعة بين الآلاف من النقاط والملايين من المستخدمين[1].

والملاحظ على هذه التعريفات أنها تركز في مفهومها للانترنت على الجانب التقني وطرق عملها.

ثانيا ــ مفهوم شبكة الانترنت في القانون: اهتم الاتجاه القانوني في تعريفه لشبكة الانترنت على رصيد القيمة الإنسانية لهذه الشبكة، ووظائفها في خدمة البشرية بالإضافة إلى جانبها التقني وذلك كما يلي:

شبكة الانترنت هي: شبكة دولية من الحواسيب المترابطة والمتصلة، وتعد من أهم وسائل الاتصال الحديثة التي ليس لها حدود إقليمية[2].

وجاء في تعريف آخر أنها: شبكة عنكبوتية تصل بين شبكات الحواسيب المتصلة عبر الدول، وتسمح بتبادل المعلومات عبرها بين الأفراد والمؤسسات والشركات وذلك عن طريق استخدام بروتوكول *TCP/IP.[3]

المطلب الثاني: تاريخ نشأة الانترنت وخصائصها

الفرع الأول ــ مراحل نشأة الانترنت:

يعود تاريخ نشأة الانترنت إلى سنة 1962 لما كانت هيئة الدفاع الجوي الأمريكية تفكر في بناء شبكة معلوماتية للاتصالات، تؤمن لها دورة المعلومات وتعتمد على نظام لا مركزي ولا تتأثر بالهجمات النووية المتوقعة، وفي السنة نفسها اقترح الباحث بول باران Paul Baran أسلوبا لاستمرار تبادل البيانات بين الحواسيب في حال تعطل بعضها إثر وقوع الحرب وذلك بتطبيق فكرتين: الأولى هي تجزئة كل رسالة إلى أجزاء صغيرة، والثانية الترابط غير المركزي بين جميع الحواسيب بحيث يمكن

---

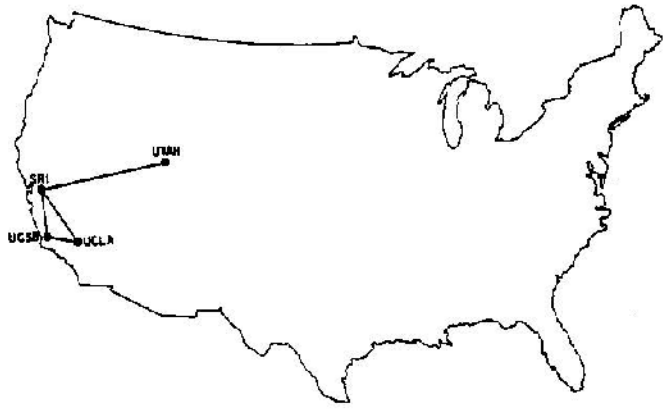
(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

إرسال كل جزء من هذه الرسائل عبر سبل مختلفة لتنتهي جميعها عند المستقبل النهائي الذي يقوم بجمعها في رسالة واحدة كما كانت عليه سابقا[1].

وفي أواخر سنة 1968م تحقق إنشاء شبكة معلوماتية للاتصالات تعتمد على نظام غير مركزي تابعة لوزارة الدفاع الأمريكية، وأطلق على هذه الشبكة إسم *ARPANET والتي هدفها ربط مختلف مراكز البحث العسكرية الأمريكية، وفي عام 1969م فتح مركز البحث القومي الأمريكي شبكته للباحثين المدنيين من أجل الاستفادة من الأبحاث العلمية العسكرية في الشؤون المدنية، وقد انضم إلى الشبكة أربعة هيئات جامعية وهي: معهد ستون فورد، وجامعة لوس أنجلوس، وجامعة سنتا بربرا، وجامعة أوتا[2].



الشكل (02) يبين شبكة آربانت البحثية على الخريطة عام 1969م[3]

ولقد اقتصرت الشبكة آنذاك على الاتصالات بواسطة البريد الإلكتروني الذي استخدمته الهيئات الجامعية في عقد اللقاءات والندوات العلمية مستفيدة بذلك من فارق المسافات، وفي سنة 1972 توسعت الشبكة إلى ما يقارب أربعين حاسوبا عبر الجامعات الأمريكية، واعتبارا من 1987م تزايد عدد المتعاملين مع هذه الشبكة خصوصا بعدما تحررت لتشمل جميع المجالات الاقتصادية والاجتماعية والسياسية والثقافية[4]، حيث بلغ عدد الحواسيب المرتبطة بالشبكة عشرة آلاف حاسوب (10000) حاسوب ليصل في سنة 1989 إلى مائة ألف حاسوب (100000)، وفي سنة 1991 تم

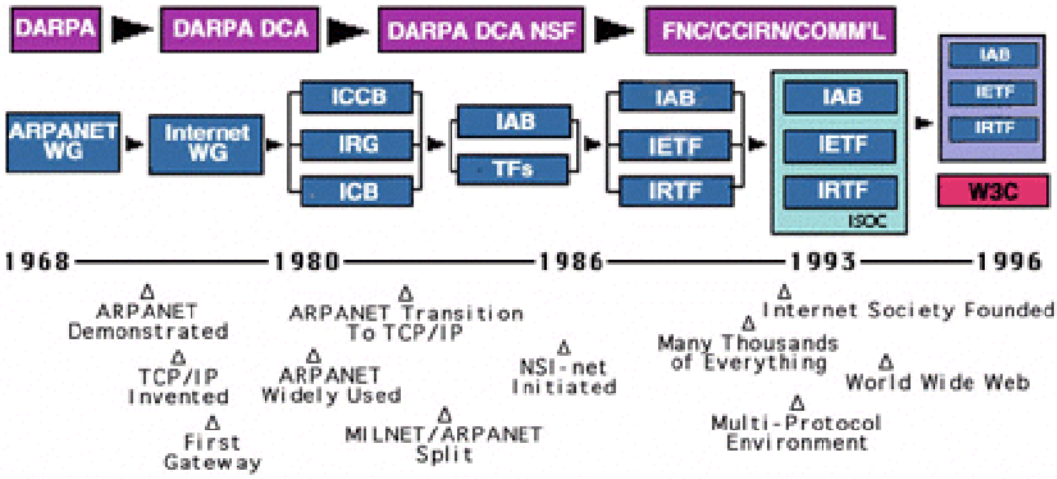
---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الإعلان عن النسيج العالمي World Wide Web (www) وتعميمه، وهذا بعد إلغاء الشبكة البحثية "آربانت"، وقد بلغ عدد الحواسيب المرتبطة بالشبكة في سنة 1996م 10 ملايين حاسوب، وفي سنة 2000م انتشرت الانترنت على المستوى العالمي وذلك بعدما أصبحت البنية التحتية للانترنيت شبه ثابتة وأصبح التطور واضحا أكثر على مستوى البرمجيات والخدمات التي تقدمها الشبكة، فتطورت صفات الانترنت الثابتة إلى صفحات ديناميكية تعتمد على لغات البرمجة المختلفة، والتي مهدت إلى ظهور جيل جديد من خدمات الانترنت ومواقع التواصل الاجتماعي كالفيسبوك والتويتر وغيره[1].



شكل(03) يوضح المراحل التاريخية لتطور شبكة الانترنت[2]

أما في وقتنا الراهن فقد أصبحت كل من الانترنت والشبكات الاجتماعية والهواتف الذكية من بين أهم الأشياء التقنية التي تشهد تطوراً كبيرا وزيادة كبيرة من حيث نسب اعتمادها أو استخدامها من قبل المستخدمين على الصعيد العالمي، وفي هذا الجانب قامت مؤسسة "We Are Social" المهتمة بشؤون الانترنت بإصدار تقرير يسلط الضوء على حالة استخدام هذه الأخيرة، حيث جاء في تقرير لها صدر سنة 2014م بأنه بلغ عدد مستخدمي الانترنت في كل مناطق العالم 2.5 مليار مستخدم.[3]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

الفرع الثاني: فوائد شبكة الانترنت واستخداماتها[1]

من الصعب حصر فوائد الانترنت لعمومها في جميع النواحي الإعلامية منها والتجارية والأكاديمية والطبية والاجتماعية والصناعية والزراعية والسياسية.. كما لم يقتصر استخدام الانترنت على المختصين في المعلوماتية بل يستخدمها الأكاديميون والباحثون، والأطباء، و الإداريون، و رجال الأعمال، والسياسيون، والإعلاميون، والتربويون، وعامة الناس، وذلك وفق أغراض عديدة منها على سبيل المثال: الحصول على البرمجيات، وتبادل المعلومات، والمراسلة بالبريد الإلكتروني، والاستفادة من قواعد المعلومات، ونشر الإعلانات و التسويق الإلكتروني، وعقد الندوات المتخصصة إلكترونيا، ومتابعة أخبار العالم ، وأداء الأعمال التجارية والحكومية وغيرها، ومن أبرز استخداماتها ما يلي:

أولا ــ الاتصالات الإلكترونية:

هي عبارة عن تطبيقات خدمية توفر التواصل عن طريق المحاورة والمراسلة الإلكترونية بين مستخدمي الانترنت، ومن أهمها:

1 ــ البريد الإلكتروني: وهو التطبيق الأكثر استخداما على شبكة الانترنت، حيث يُمكن المستخدمين في كل أقطار العالم من تبادل الرسائل الإلكترونية فيما بينهم بسرعة لا تقارن بالبريد التقليدي وبتكلفة رمزية، كما يتم من خلاله إجراء العقود الإلكترونية والمراسلات التجارية مهما كان عددها أو حجمها وهو ما وفر على الهيئات التجارية والمالية مبالغ طائلة كانت تدفع مقابل خدمات البريد العادي أو أجهزة الفاكس.

2 ــ القوائم البريدية: يتيح تطبيق القوائم البريدية إمكانية إرسال رسالة إلكترونية إلى أكبر عدد من الأشخاص في آن واحد بغرض مناقشة موضوع معين على سبيل المثال، أو نشر خبر ما ونحوه، وتتميز القوائم البريدية بأنه لكل قائمة عنوان بريدي موحد ترسل إليه الرسائل الإلكترونية ومن ثم يتم توزيعها على المشتركين في القائمة، وعملية الاشتراك في إحدى هذه القوائم أو الانفصال عنها لا يتعدى إرسال طلب إلكتروني إلى العنوان الخاص بالاشتراكات في قائمة معينة، وتتوفر الانترنت على مئات الآلاف من القوائم البريدية التي تناقش موضوعات عدة في شتى المجالات العلمية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والتقنية والأدبية والاجتماعية والسياسية والدينية والتربوية والتعليمية وغيرها.

3 ــ المجموعات الإخبارية News groups : يمكن تمثيل المجموعات الإخبارية بالمنتديات التي تضم أفرادا من مختلف أنحاء العالم يجمعهم اهتمام مشترك بموضوع معين، فهي بمثابة نواد افتراضية للنقاش وتبادل الآراء والمعلومات تمكّن أي مشترك فيها من نشر أو قراءة المقالات المنشورة عليها، ولتسهيل انتقاء المجموعة الإخبارية فإنها تصنف وفق فئات رئيسية على سبيل المثال: الكمبيوتر(Comp) ، العلوم (Sci)، الاستجمام (Rec) ، موضوعات بديلة (Alt) ، موضوعات اجتماعية (Soc) ، موضوعات ساخنة (Talk) ، موضوعات تجارية (biz) ، والموضوعات التنظيمية الخاصة بشبكة الانترنت (News Usenet) ، ولقد بلغ عدد هذه المجموعات (أكثر من 40 ألف مجموعة إخبارية) والعدد يتزايد باستمرار.

كما تمكن مستخدمي الانترنت من الانتساب إلى ما يشاءون من المجموعات الإخبارية بمنتهى السهولة، حيث يحصلون بصفة تلقائية على كافة الرسائل التي ينشرها أعضاء المجموعة المنتقاة، كما يمكنهم مخاطبة جميع أعضاء المجموعة عن طريق الرسائل الإلكترونية[1].

4 ــ التحاور الآني (المحادثة): هي عبارة عن تطبيقات تتيح لمستخدميها إمكانية التحاور الآني عن بعد باستعمال لوح مفاتيح و شاشة الحاسوب، حيث تقرب أطراف الحوار وكأنهم في مكان واحد، ومن أمثلتها تطبيقات Talk و Chat. فمن خلال المحادثة الآنية يستطيع المستخدم الدخول لإحدى ساحات الحوار ومن ثم البدأ بمشاركة الآخرين آراءهم بواسطة إرسال واستقبال الرسائل سواء كانت نصية أو مرئية أو مسموعة، كما تستخدم هذه التقنية أيضا من قبل بعض الهيئات للتحاور الإلكتروني بالصوت والصورة ولعقد اجتماعاتها عن بعد.

5 ــ مؤتمرات الفيديو Video Conferencing : عند ظهور الانترنت بدأ الطموح العلمي في مجال الاتصالات يقفز من مرحلة الاكتفاء بالصوت إلى مرحلة طلب الصوت و الصورة الأمر الذي أدى إلى ابتكار ما يعرف بـــ"مؤتمرات الفيديو" (Video Conferencing)، وهي عبارة عن اتصال سمعي بصري يجري في وقت واحد بين أطراف متفاعلة معاً في مواقع مختلفة حيث يمكن من خلال تلك المواقع استعمال الشبكة في التحاور معاً أو مع الموقع الرئيسي باستغلال وسائط الحاسوب السمعية

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والمرئية مما يتيح للمتحاورين في المواقع المختلفة توجيه الأسئلة والاستفسارات والتعليقات إلى الموقع الرئيسي واستقبال الإجابات والاستفسارات آنيا.

وتُعد تكنولوجيا مؤتمرات الفيديو من أهم المستحدثات التكنولوجية التي أتاحت بعداً جديداً من أبعاد التعلم التفاعلي وذلك لتعدد فوائدها العامة والتعليمية، حيث تُستخدم في توصيل التعليم من بعد وتحسين الاتصال بين عناصر المنظومة التعليمية[1].

ثانيا ــ تطبيقات المشاركة وتبادل الموارد:

هي تطبيقات تتيحها الانترنت لتمكين المستخدمين من تبادل الموارد فيما بينهم أو المشاركة فيها عن بعد، ومن أمثلة ذلك نقل الملفات، أو الدخول عن بعد، أو استخدام النسيج العالمي:

1 ــ نقل الملفات: تعد خدمة نقل الملفات إحدى الخدمات الأساسية في الانترنت التي تساعد المستخدم في نقل الملفات بين جهازه وأي جهاز آخر يملك تصريح الدخول إليه، أو أن يكون الدخول عن طريق نظام (Anonymous FTP) الذي توفره معظم الجهات المرتبطة بالانترنت كوسيلة لتسهيل نقل الملفات، حيث يسمح لأي مستخدم الدخول برمز استخدام موحد وهو عبارة عن ("anonymous") والمتعارف عليه أن تكون كلمة السر هي الرمز البريدي للمستخدم.

2 ــ الدخول عن بعد إلى الحواسيب: هي خدمة تسمح للمستخدم بالدخول إلى أي حاسوب مرتبط بشبكة الانترنت من خلال جهازه الخاص حيث يصبح بإمكانه تشغيل البرامج وتصفح الملفات المخزنة على ذلك الحاسوب، ويتطلب ذلك تصريح بإذن الدخول المعروف برمز الاستخدام، أو أن يكون الحاسوب مجهزا للاستخدام العام كفهارس المكتبات و قواعد المعلومات، ومن التطبيقات المستعملة في هذه الخدمة برنامج (telnet) و (rlogin) اللذان يتيحان للمستخدم إمكانية الدخول من بعد إلى الأجهزة عن طريق الانترنت.

3 ــ تصفح شبكة النسيج العالمي: تقدم الانترنت واجهة موحدة لجميع الخدمات حيث يسمح للمستخدم تصفح المعلومات و عرضها على جهازه من غير أن يكون له أدنى معرفة بطريق التخزين أو النقل، ومن أشهر هذه التطبيقات شبكة النسيج العالمي (الويب WEB) التي يستخدم فيها تقنية النصوص المترابطة لإتاحة إمكانية التنقل بين المعلومات المتوفرة على الشبكة بدون معرفة مكان

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

نشر تلك المعلومات، و لقد ساهمت هذه الخدمة في انتشار استخدام الانترنت والزيادة المطردة لأعداد المستخدمين نظرا لما توفره من سهولة في عرض و نقل المعلومات بشتى صورها.

ويستخدم في شبكة النسيج العالمي تقنية الخادم والعميل، حيث يعمل متصفح الشبكة كعميل لخادم الشبكة أو مقدم المعلومات، ويسمح للعميل بطلب الخدمات المتوفرة على شبكة الانترنت أو تشغيل برنامج متوفر عند الخادم باستخدام مجموعة من قواعد التخاطب بين الخادم والعميل، كما أن لكل صفحة من صفحات النسيج عنوان فريد على الشبكة يمكن تحديده باستخدام محدد عنوان الخدمة (URL) وهو صيغة مقننة لتحديد نوع وعنوان الخدمة على الشبكة[1].

ثالثا ــ تطبيقات البحث عن الموارد:

إن الكم الهائل والمتزايد من المعلومات على الانترنت جعل البحث عن معلومة ما أمر بالغ الصعوبة، وهو ما استدعى توفير بعض التطبيقات الخدمية التي تساعد المستخدم على تحديد مكان المعلومات المطلوبة على الشبكة وعرضها على جهازه في وقت قياسي، ومن بينها على سبيل المثال:

1 ــ البحث عن عناوين البريد الإلكتروني للأشخاص: فإذا تعذر معرفة عنوان البريد الإلكتروني لأحد الأشخاص أو الهيئات، فإنه بإمكان التطبيق Netfind البحث عن عنوان البريد الإلكتروني وذلك عن طريق إدخال ألفاظ دلالية لاسم الشخص أو الهيئة محل البحث ويتكفل البرنامج التطبيقي بباقي المهمة.

2 ــ البحث عن ملفات معينة: توفر الانترنت الملايين من الملفات التي يمكن الحصول عليها عن طريق الخدمة المجانية(Anonymous FTP) ، ويتطلب نقل أي ملف معرفة عنوانه الإلكتروني، ولتسهيل عملية البحث فإن الانترنت توفر خوادم خاصة لإنشاء وتخزين قوائم بأسماء الملفات المتوفرة على الخوادم المجانية (Anonymous FTP)، كما يتم تحديث هذه القوائم آليا بين حين و آخر، ولا تتطلب عملية البحث إلا استخدام أحد التطبيقات المعروفة على الانترنت كتطبيق (archie) الذي يكتشف مكان الملف في وقت قياسي.

3 ــ البحث عن المعلومات: توفر شبكة الانترنت مجموعة كبيرة من نظم البحث التي من أشهرها ما يسمى بأدلة الانترنت وفهارس الانترنت، وكلاهما يختلف عن الآخر في طريقة جمع

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المعلومات وفهرستها وطريقة البحث فيها.

فتقوم أدلة الانترنت بتصنيف اغلب محتويات الانترنت حسب موضوعاتها على شكل سرد هرمي مشابه للتصنيف المستخدم في المكتبات، ويكون التصنيف في الغالب يدويا حيث يقوم العاملون على الأدلة بتتبع مواقع نشر المعلومات بطرق بحث مختلفة وتسجيل موضوعات وأماكن نشر تلك المواقع وملخص لمحتوياتها، ويكون الدليل في الغالب دقيقا في تصنيف المعلومات، و لكنه لا يعطي رصدا لكامل محتويات الانترنت نظرا لاعتماده على التحديث اليدوي الذي يكون في الغالب مكلفاً في الجهد والوقت، ومن أشهر الأدلة على شبكة الانترنت دليل الياهو (www.yahoo.com) الذي أنشئ في أواخر عام 1994م حيث يرصد أكثر من ثمانمائة ألف موقع وهو متوفر في نسخ متعددة بلغات مختلفة وفي أماكن متفرقة من العا لم.

أما فهارس الانترنت فتعطي رصداً آلياً للتعابير والمفردات الواردة في المعلومات المنشورة على الشبكة مع بيان أماكن نشرها، وتتيح هذه الفهارس إمكانية البحث باستخدام طرق مختلفة، كما تتميز بتغطية كبيرة للمعلومات مقارنة بأدلة الانترنت، إضافة إلى توفرها على واجهه تخاطبيه معيارية، ومن أشهر تلك الفهارس نظام ألتا فيستا (www.altavista.com) الذي أنشئ في نهاية عام1995م ، وكذلك نظام هوت بوت (www.hotbot.com) الذي أنشئ عام 1996م.[1]

4 ــ النشر: يتم تصميم ونشر الصفحات على شبكة الانترنت إما باستخدام لغة ترميز النصوص المترابطة (HTML) مباشرة، أو باستخدام بعض برامج التصميم والنشر التي تساعد المستخدم في تصميم ونشر الصفحات على الانترنت بدون سابق معرفة بلغة (HTML) ، ولقد ساهمت خاصية نشر المعلومات على شبكة الانترنت إلى سرعة غير مسبوقة في ضخ معلومات هائلة ومتنوعة الأمر الذي ساعد المستخدمين في الوصول إلى أي معلومة يريدونها بطرق يسيرة سواء كانت تلك المعلومات على صيغة نصوص أو صور، أو ملفات صوتية، أو سمعية بصرية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الثالث:

المجرم المعلوماتي وعلاقته بالجريمة الإلكترونية

المبحث الأول: المفهوم العام للمجرم وسيكولوجيته

المبحث الثاني: سمات المجرم المعلوماتي وتصنيفاته

المبحث الثالث: المجرم المعلوماتي والهندسة الاجتماعية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

تمهيد:

من الناحية النظرية لا تثبت صفة المجرم في شخص ما بدون أن يصدر منه سلوكا إجراميا، وفي العادة عند الحديث عن الجريمة فإنها تنسب إلى فاعلها أكثر مما يشار إليها كفعل، فنجد مثلا لفظ اللص والنصاب والمحتال والسفاح يستعمل أكثر مما يستعمل لفظ السرقة والنصب والقتل لعدم إلمامها بجزئيات نموذج الجريمة كما هو معروف في القانون الوضعي، بينما العبارات الأولى تصور الجريمة وتعطي في الوقت نفسه صورة الإنسان الذي يقترفها[1].

ولذلك لم يؤثر ارتباط الجريمة المعلوماتية بالحاسوب على تمييزها عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا في تمييز المجرم المعلوماتى عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامى النمطي، وهذا ما سوف أتطرق له موضحا أهم سمات المجرم المعلوماتي ودوافعه الإجرامية وأنماطه.

المبحث الأول: المفهوم العام للمجرم وسيكولوجيته

المطلب الأول: تعريف المجرم في اللغة والاصطلاح

الفرع الأول ــ التعريف اللغوي للمجرم:

المجرم لغة؛ الذي ارتكب جُرما يستحق عليه العقاب، وأجرم يُجرم، إجراما، فهو مجرم، وأجرم الرجل: ارتكب ذنبا أو جنى جناية، وأجرم عليهم وإليهم: جنى جناية، وأجرم النخل والتمر: حان جرامُه، وأجرم الرجل: أكسبه جُرما، وأجرم الشخص: ألصق به الجُرم أو الذنبَ مؤامرة مجرمة، وأجرم شريكه وبرأ ساحته.[2]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني ــ تعريف المجرم في الاصطلاح الفقهي:

لم يحدد تعريف خاص بالمجرم اصطلاحا وإنما ربط الفقه المجرم بصفات الجريمة، والجريمة في الفقه الإسلامي هي: " إتيان فعل محرّم معاقب على فعله، أو ترك فعل محرّم الترك معاقب على تركه، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه "[1].

الفرع الثالث ــ تعريف المجرم في القانون الوضعي:

المجرم في القانون؛ هو من أتى فعلاً يُعدّ في نظر القانون جريمة سواء كان هذا الفعل إيجابيا أم سلبيا، وصدر ضده حكما قضائيا باتاً أو مبرماً بإدانته[2].

فمن الوجهة القانونية كي يعد الشخص مجرما لابد من توفر شرطين هما:

1 ــ أن يرتكب الشخص تصرفا أو فعلا (أو امتناعا عن فعل) يعد جريمة وفقا لنص التجريم القانوني فلا جريمة إلا بنص القانون، مع إرادته لهذا الفعل وعلمه بما يترتب عليه من نتائج.

2 ــ ثبوت إدانته أمام المحاكمة بارتكاب الجريمة، فلا يكفي اعتبار الشخص مجرما في نظر القانون أن يرتكب فعلا مجرّماً وفقا لنص التجريم، بل لابد أن يدان أمام القضاء بارتكاب هذه الجريمة بحكم قضائي بات تطبيقا للقاعدة الأساسية في التشريعات الجزائية الإجرائية والتي تقضي بأن الأصل في الإنسان البراءة إلى أن تثبت إدانته بحكم قضائي قطعي.

ولقد تعرض المفهوم القانوني للمجرم إلى النقد من بعض الفقهاء ذوي الاهتمام بالدراسات الإجرامية حيث استندوا في ذلك إلى العديد من الأسباب التي تؤيد وجهة نظرهم، أبرزها:

1 ــ هناك طائفة من الأفعال المجرّمة قانونا ذات طابع إداري، ولا يبرر وصف مرتكب أيا منها بأنه مجرم كمخالفات قانون المرور فهي لا ترقى بمرتكبها إلى مصاف المجرمين ما دام أن هذا السلوك لا يعبّر عن عدم اكتراث حقيقي للنصوص القانونية المطبقة في المجتمع[3].

2 ــ هناك الكثير من الأفعال التي يجرّمها القانون الجزائي ويعاقب عليها لا تنم عن خطورة إجرامية ولا تعبر عن أي سلوك إجرامي، بل يعدّ بعض مرتكبيها في مصاف الأبطال وليس المجرمين، كالجرائم السياسية والاقتصادية وجرائم الرأي في نظر القانون والجرائم ذات الصلة بحياة الفرد

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الشخصية والمرتبطة بحريته، في حين يعد الكثير من أفعال الناس في دائرة الجرائم والانحرافات بالرغم من عدم تجريم القانون لها كالتعامل بالربا، والإدمان على تعاطي الكحول والمخدرات وهي أفعال تشكل خطورة بالغة تستدعي من المشرع تجريمها [1].

المطلب الثاني: مفهوم المجرم في علم الإجرام

يرى علماء الإجرام أن التعريف القانوني للمجرم لا يفي بالغرض المنشود من وراء دراسته، فهم لا يقتصرون في دراستهم على من يثبت ارتكابه للجريمة بحكم الإدانة فحسب بل يتوسعون في المقصود من اصطلاح المجرم فيدرجون في دراساتهم أولئك الذين ألقي القبض عليهم ويخضعون للتحقيق، والمجرمين الذين تجري محاكمتهم أمام القضاء، كما يتوسع بعض علماء الإجرام في المقصود بالمجرم الحقيقي أنه المجرم الذي ارتكب جريمة سواء أكان في السجن أم خارجه، وهذا باعتبار أن المجرم ليس من وقع تحت طائلة القانون وثبتت إدانته فقط، بل هناك الكثير ممن يرتكبون الجرائم و لم تطلهم يد العدالة بعد، وحجتهم في ذلك أن علم الإجرام لا يرتب في نتائج بحوثه تلك النتائج أو الآثار الخطيرة التي يرتبها القانون الجنائي على ثبوت صفة المجرم لشخص ما[2].

واستنادا إلى ذلك فإن مفهوم المجرم عند معظم علماء الإجرام هو "الشخص الذي يرتكب جريمة ينص عليها القانون" فيكفي لاعتبار الشخص مجرما ارتكابه فعلا مخالفا للقانون سواء أدانه القضاء أم لم يدنه بعد[3].

كما أن المجرمين الذين يتناولهم علم الإجرام بالدراسة ليسوا على نفس الدرجة من الإدراك والتمييز، فهم ينقسمون لأكثر من طائفة بحسب تكوينهم العضوي والنفسي والعقلي مما يؤثر في مسؤولياتهم الجنائية، وعلى هذا الأساس يميز بين طائفتين من المجرمين هما: المجرمون الأسوياء والمجرمون غير الأسوياء.

ويقصد بالمجرمين الأسوياء، من تتوافر فيهم كافة شروط المسؤولية الجنائية لخلوّهم من العوارض التي تؤثر على سلامة إدراكهم واختيارهم وبالتالي فهم يسألون جنائيا عن تصرفاتهم.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أما المجرمين غير الأسوياء فهم على نوعين: مجرمون مجانين تنعدم مسؤوليتهم الجنائية بسبب فقدان العقل، كما تسقط عنهم كل عقوبة مقررة في القانون، إلا أن ذلك لا يحول دون اتخاذ بعض التدابير الاحترازية تجاههم لمواجهة خطورتهم الإجرامية، والنوع الثاني هم المجرمون الشواذ، وهم المصابون بخلل جزئي في تكوينهم العقلي أو النفسي، أو العضوي، وهذا الخلل لم يصل إلى الحد الذي تنعدم فيه أهليتهم الجنائية، إذ يتمتعون بقدر من الإدراك والاختيار أقل من المجرمون الأسوياء، ولذلك تقرر بعض التشريعات لهذه الطائفة مسؤولية جنائية مخففة.[1]

و يصنف علم الإجرام المجرمين الأسوياء إلى ثلاث مترادفات لكل منها نظرية مختلفة، وهو ما لخصته في الفروع التالية:

الفرع الأول: المجرم المحترف

هي تسمية أمريكية الأصل في مجال علم الجريمة، جاء مصدرها كرد فعل بعض علماء الاجتماع الذين يرفضون فيها تفسير ظاهرة اعتياد الإجرام على أساس خصائص فردية بدلا من اعتبار الاعتياد كدور يحدد اجتماعيا مثل باقي الأدوار، وقد وضع هؤلاء عددا من التصنيفات للمجرم العائد وحاولوا ربط كل تصنيف بخلفيات اجتماعية معينة، لكن ثبت عيب هذه التصنيفات بأنها متداخلة وغير مستقلة ولا تخدم غرض فهم ظاهرة تكرار الإجرام على الإطلاق.[2]

الفرع الثاني: مدمنو الإجرام

كانت بريطانيا في الماضي ترحّل المجرمين إلى المستعمرات كوسيلة إجرائية للضبط الاجتماعي من أجل عزل أذاهم عن المجتمع البريطاني، وقد عرف هذا الإجراء تراجعا في عهد الملكة فيكتوريا مما ساهم في انتشار المجرمين في مدن انجلترا واستفحال ظاهرة الإجرام حيث فشلت كل أنواع العقوبات الردعية المطبقة تجاههم ولذلك صنف هؤلاء المجرمين بـــ (معتادي أو مدمني الإجرام) وقد صدرت عدة تشريعات في كيفية التعامل معهم لكن دون جدوى[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثالث: المُدان العائد

يقصد به المجرم الذي أدين في جريمة حديثة بعد أو أثناء قضائه للحكم الذي صدر ضده في جرائم سابقة، وقد ظهر هذا المصطلح في إنجلترا خلال سنة 1857م عند إنشاء ما يسمى بنظام سجلات الشرطة والسجون حيث استعملت السجلات الجنائية في المحاكم كأساس ثانوي وليس رئيسيا في فرض الأحكام ويعود ذلك إلى التباين الظاهر في مستويات الدقة والموضوعية لدى الشرطة من مقاطعة إلى أخرى، وقد استغل البعض هذه السجلات في إثبات وجود طبقات اجتماعية مجرمة Class Criminal في انجلترا مما أثير حولها تخوف كبير إلى أن أصبحت كابوسا يقلق راحة الإنجليز في القرن التاسع عشر[1].

وما يفهم من خلال هذه التعريفات أن مفهوم المجرم يرتبط بالفعل سواء كان إيجابيا أم سلبيا.

المبحث الثاني: سمات المجرم المعلوماتي وتصنيفاته

يعد المجرم المعلوماتي وليد التطور الهائل الذي عرفته تكنولوجيا المعلومات والاتصالات وقد أصبح يشكل خطرا كبيرا على اقتصاد البلاد وأمنها، كونه يسخر في جرائمه وسائل التكنولوجيا الحديثة كالحاسوب وشبكة الانترنت ووسائل الاتصال، كما يقوم بأفعال إجرامية ضد نظام الحاسوب نفسه، أو يسطو على البنوك مستعينا بأنظمة الحاسوب، أو يتحايل على الحواسيب مستعينا بحاسوب آخر وغير ذلك من صور الجرائم المتعددة في هذا المجال، الأمر الذي جعل من الصعوبة تحديد سمات معينة للمجرم المعلوماتي [2] حيث أن جانبا من الفقه الجنائي يرى بأن المجرم المعلوماتي يمثل بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة بذاتها، فهو من ناحية يعتبر مجرما " ذكيا"، ومن جهة أخرى إنسانا اجتماعيا بطبيعته.

ولذلك يتعين البحث في سماته ودوافع ارتكابه للجرائم الإلكترونية وأنماطه من خلال المطالب التالية:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الأول: سمات المجرم المعلوماتي[1]

قد يتطابق المجرم المعلوماتي مع المجرم التقليدي من حيث تجريم الفعل الذي يصدر من كليهما نتيجة الضرر الذي يلحقانه بالضحايا سواء كانوا معنويين أو طبيعيين، لكن يختلف المجرم المعلوماتي عن التقليدي بسمات تميزه عن غيره من المجرمين التقليديين، ومن أبرزها ما يلي:

1 ــ المجرم المعلوماتي مجرم متخصص: فقد ثبت في كثير من القضايا أن الجرائم الصادرة من مجرمين معينين لا تخرج عن دائرة التكنولوجيا الحديثة، إذ كلها تتعلق بالحواسيب والمعلومات والشبكات، وهو ما يعني أنهم تخصصوا في هذا النوع من الجرائم.

2 ــ المجرم المعلوماتي من المجرمين العائدين للإجرام: حيث ثبت في العديد من القضايا عودة الكثير من مجرمي المعلومات إلى ارتكاب جرائم معلوماتية أخرى انطلاقا من الرغبة في سد الثغرات التي أدت إلى اكتشافهم وتقديمهم إلى المحاكمة في المرات السابقة، وقد ينتهي بهم الأمر إلى تقديمهم مرة أخرى إلى المحاكمة.

3 ــ هو من المجرمين المحترفين: فارتكاب الجرائم المعلوماتية لا يسهل على الأشخاص الهواة ــ إلا نادرا ــ نظرا لما يقتضيه هذا النوع من الجرائم من العلم والدقة والتخصص في هذا المجال، حيث كثيرا ما يجابه المجرم عقبات التغلب على أنظمة الحماية التي تصادفه وهي من صنع متخصصين أكفاء في مجال المعلوماتية.

4 ــ هو من المجرمين الأذكياء: يذكر في العادة أن الإجرام المعلوماتي هو إجرام الأذكياء لكن ليس القصد من ذلك أن المجرم التقليدي يتميز بالغباء، إنما الإجرام المعلوماتي يستدعي التميز في الذكاء ليتغلب على كثير من العقبات التقنية التي تواجهه في ارتكاب جرائمه، وبينما نجد الإجرام التقليدي يميل إلى القوة والعنف المادي فإن اختراق الحواسيب أو المواقع الإلكترونية أو إتلاف الأنظمة ليس بحاجة إلى سلوك عنيف، بل ينشأ من تقنيات التدمير الناعمة Sabotage soft كالتلاعب بالمعلومات أو الكيانات المنطقية أو البيانات مما يؤدي إلى تدميرها كليا أو إتلافها جزئيا أو تشويهها[2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

5 ــ المجرم المعلوماتي لا يستعمل العنف المادي في جريمته: فلا يلجأ إلى العنف في ارتكاب الجريمة كما هو الحال لدى المجرم التقليدي لأنه لا يواجه الأشخاص الطبيعيين أثناء ارتكاب الجريمة وإنما يواجه أشخاصا معنويين الأمر الذي يستبعد اللجوء إلى العنف كاستعمال السلاح الأبيض وغيره للتملص ممن يصادفه.

6 ــ المجرم المعلوماتي من المجرمين الذين يتكيفون اجتماعيا: ففي كثير من الحالات يعرف على المجرم التقليدي حالة من العداء السافر تجاه المجتمع الذي يعيش فيه عكس المجرم المعلوماتي الذي يتكيف اجتماعيا، ويساعده في ذلك ارتفاع نسبة الذكاء العلمي الذي يتصف به مما يخفي صفة الجريمة عنه في الوسط الاجتماعي، وهذا لا يعني التقليل من شأنه لأن خطورته الإجرامية قد تكون أكثر حدة إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه[1].

وفي هذا السياق تذكر بعض الدراسات المتخصصة بأن الإجرام المعلوماتي تمخض عن عوامل مستحدثة في أذهان مرتكبيه حيث يلجأ العديد منهم إلى ارتكاب هذه الجرائم بدافع اللهو أو لمجرد إظهار تفوقهم على الآلة، أو على البرامج المخصصة لأمن النظم المعلوماتية، وهذا بقصد التفاخر بأنفسهم وأن يظهروا لضحاياهم ضعف أنظمتهم[2]. لكن هذا السلوك غير الواعي يمكن أن يلحق الضرر بالمجتمع حتى ولو لم يظهر أي عداء له، ودليل ذلك ما نشهده من نماذج إجرامية عديدة كانت نتيجة نوايا حسنة وقعت من أحداث صغار أو بالغين وكانت آثارها جد خطيرة، حيث تم استغلال عقولهم و تجنيدهم ضمن عصابات الجريمة المنظمة على شبكة الانترنت، كما استغلوا في سرقة الأموال والتلاعب في الحسابات وأرقام بطاقات الائتمان وغيرها من الأعمال المضرة بالفرد والمجتمع[3].

المطلب الثاني: دوافع الجرائم الإلكترونية

لقد أجريت دراسات عديدة في مجال علم الإجرام تتعلق بدوافع المجرمين في ارتكاب جرائمهم خاصة منها الجرائم الإلكترونية، وتوصل الباحثون إلى أن هناك دوافع يراها مرتكبي الجريمة منطقية ليبرروا تصرفاتهم ومن أبرزها ما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أولا ــ إثبات التفوق العلمي: يلجأ العديد من المهتمين إلى إثبات التفوق العلمي من خلال التحدي الفكري أثناء استخدامهم للحاسوب وإثبات قدراتهم على اختراق أنظمة الحواسيب والدخول عليها، وهو دافع جعل الكثير يقومون بمثل هذه الأفعال على الرغم من عدم توافر نية ارتكاب الجرائم. وقد ثبت أن أغلب من يتصرفون بدافع إثبات التفوق العلمي هم الصبية والشباب المعروفون باسم صغار نوابغ المعلوماتية، حيث أن همهم الدائم هو اكتشاف الجديد من البرامج والتعامل معها مع إثبات تفوقهم العلمي عن طريق تخطي حاجز الحماية لهذه البرامج وتحطيمها غير مبالين بما يحدثونه من مشاكل[1] .

ثانيا ــ الانتقام: يعد الانتقام من أخطر الدوافع التي تحث الشخص على ارتكاب الجريمة، فهذا الدافع غالبا ما يصدر من شخص يملك معلومات كبيرة عن الضحية سواء كان فردا أو هيئة أو مؤسسة كالمكان الذي يعمل به على سبيل المثال حيث يرتكب جرمه بدافع الانتقام نتيجة لمظلمة يريد دفعها وهي صورة قد تكون أقل بأس من الصور الأخرى التي يغذيها دافع الانتقام[2].

ثالثا ــ ارتكاب الجرائم كوسيلة للتسلية أو المزاح: أحيانا تكون التسلية أو المزاح من الدوافع التي تجعل الشخص يقوم بتصرفات ــ عن حسن النية ــ فتنتج عنها جرائم معينة كمسح البيانات أو الملفات من جهاز الضحية والتي قد تكون بالغة الأهمية لكن الفاعل لا يدري أن حقيقة تصرفه هي جريمة إتلاف وتخريب متعمد[3].

رابعا ــ الشعور بالنقص: وهو من العوامل المؤثرة في إقدام المجرم على ارتكاب جريمته، فقد يكون هذا الشعور له علاقة بالناحية الفسيولوجية أو النفسية أو العلمية للجاني مما يؤدي إلى شعوره بأنه أقل مستوى من الآخرين، فيحاول إثبات ذاته وتغلبه على هذا النقص بإظهار تفوقه في مجال آخر تعويضا عن العجز الذي يتملكه فيقدم على ارتكاب جريمة ما تضر بالغير وتجعلهم عاجزين هم أيضا عن التصدي لها كتعطيله لأنظمة الحواسيب مثلا [4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

خامسا ــ دوافع سياسية: وهي دوافع لها صلة بالتوترات السياسية كالتي تعرّض لها العالم بعد حوادث سبتمبر وما أعقبه من غزو لبعض البلدان العربية والإسلامية والتوترات الحاصلة في العالم، حيث ظهرت أنشطة عشوائية أو منظمة من جهات معينة تمارس العديد من أنواع الجرائم الإلكترونية.

وفي هذا الشأن كشفت شركة فيريزون Verizon العالمية للاتصالات وتكنولوجيا المعلومات في تحليل سنوي لحوادث اختراق المعلومات على الانترنت عن ارتفاع كبير في عدد الهجمات الإلكترونية ذات الدوافع السياسية[1]، وجاء في تقريرها أن 58 بالمائة من كل البيانات المسروقة عن طريق الاختراق سنة 2011 كان الهدف منها سياسيا، وقال ويد بيكر مدير قسم الأبحاث والمعلومات للشركة: "لقد ظل نشاط القرصنة لأغراض سياسية موجودا منذ فترة، ولكن كان بشكل أساسي يهاجم المواقع الإلكترونية، أما في عام 2012، فقد أصبح الأمر يتعلق أكثر بسرقة العديد من المعلومات من الشركات".

وأضاف بيكر: "لقد أصبحت القرصنة لأغراض سياسية أحد آليات الاحتجاج السياسي"، كما أشار إلى أنه من الصعب تطوير نظم دفاعية محددة ضد هذه الهجمات الإلكترونية لأن مجموعات القرصنة السياسية تستخدم وسائل وأساليب خاصة يتم ابتكارها لكل مناسبة بعينها[2].

سادسا ــ دوافع جنسية: إن الدوافع الجنسية غير المنضبطة تقود غالبا صاحبها في غير هدى منه أو روية، فيصبح همه الأكبر هو إشباع رغباته التي لا تنتهي ويزداد الأمر سوء عندما لا يقنع بما ألفه وتعوّد عليه من مناظر جنسية، فيلجأ إلى التوسع في ذلك للحصول على وجوه جديدة أو أشخاص قريبين منه، وبالتالي يسعى قدر المستطاع بالاختراق أو التجسس على من يقع عليهم اختياره ليفوز بما يصبو إليه من متعة[3].

سابعا ــ دوافع عقائدية: تعد العقيدة من أقوى الدوافع والقوى المحركة للأشخاص، فقد ثبت أن كثيراً من مجرمي الانترنت يبررون تصرفاتهم وفق تأويلات عقدية غريبة وأفكار سيئة، فمنهم من يحاول اختراق موقع إلكتروني بغرض إتلافه أو تعطيله بحجة أنه معاد لذلك المذهب أو الطائفة الدينية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أو بحجة تكفيرية، كما يحاول البعض منهم نشر أفكار عقائدية باطلة بغرض التضليل ونشر الفوضى وعدم الاستقرار، أو الاطلاع على أسرار الخصوم في العقيدة لفضحهم والتشهير بهم، وقد توصل الأمر إلى سب الأديان والأنبياء والاستهزاء بهم عن طريق نشر مواقع متخصصة في هذا المجال تغذيها دوافع عدة من بينها الإلحاد والعقائد الضالة[1].

ثامنا ــ الدوافع المالية: إن الرغبة في الربح السريع والحصول على المال دفع مجرمي المعلوماتية إلى سلوك طرق غير مشروعة لاختراق قواعد بيانات المؤسسات المصرفية والمالية وممارسة النصب والاحتيال عبر الانترنت بأساليب مختلفة وتقنيات متنوعة، ولقد ساهم في ذلك كثرة المنتديات والمواقع التي تقدم برامج مجانية ومعلومات بشرح وافي عن طرق الاختراق والسرقة والتجسس وهو ما ألحق ضررا كبيرا بالمؤسسات المالية بصفة خاصة، كما أثّر ذلك سلبا على تطبيقات التجارة الإلكترونية خصوصا في الدول النامية ومنها المنطقة العربية[2].

المطلب الثالث: تصنيفات المجرم المعلوماتي

يعتمد المجرم المعلوماتي في تنفيذ جرائمه على المهارة اللازمة المحصلة عن طريق الدراسة أو الخبرة المكتسبة في تكنولوجيا المعلومات، والمعرفة الكاملة بمحيط الجريمة وظروفها والوسيلة التي يتزود بها، والقدرة على ابتكار الأساليب الملائمة Ressources ، والسلطة المباشرة أو غير المباشرة في الوصول إلى المعلومات والحصول على الشيفرة Authority [3] .

وكنتيجة لتعدد دوافع مجرمي المعلومات في ارتكاب جرائمهم فقد اكتسبوا تسميات مختلفة تتوافق وتخصصاتهم في الجريمة الإلكترونية، مثل: "Carders" وهو اسم الذين يسرقون بطاقات الائتمان أو يبيعون المعلومات المتعلقة بالبطاقات المسروقة عبر الانترنت[4]، و "Phreakers" الذين يستغلون معرفتهم في تقنيات أنظمة الهواتف فيستعملونها لمكالماتهم على حساب ملاكها الأصليين[5]،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

و ''Crashers'' الذين يستمتعون باقتحام أجهزة الكومبيوتر وتدمير محتوياتها[1]، و''Cypherpunks'' هم الذين يكسرون التشفير ويدمرون أنظمة الحماية الأمنية للمعلومات [2]، و''Script Kiddies'' هم من المبتدئين الذين لهم معرفة محدودة في مجال المعلوماتية ورغم ذلك فإنهم يستخدمون برامج نصية بسيطة وأدوات رقمية متاحة على الإنترنت لإلحاق الضرر بالغير[3] ، و''Uberhackers'' وهم من أخطر الفئات لكونهم يتمتعون بكفاءات عالية، فيوظفون تقنيات جد احترافية ومعقدة من أجل التسلل إلى الأنظمة المعلوماتية وفق دوافع مختلفة قد تكون سياسية أو إرهابية وغيرها[4]، ولا يزال فضاء المعلوماتية يشهد أصناف عديدة من المجرمين يصعب حصرهم، ولذلك صنفتهم من حيث الخطورة الإجرامية وفق الفروع التالية:

الفرع الأول ــ القراصنة:

1 ــ القراصنة الهواة: Hackers [5]

هم فئة من الشباب يطلق عليهم في بعض الدراسات تسمية صغار نوابغ المعلوماتية[6]،كثيرا ما يقومون بانتهاكات غير مسموح بها في العديد من الأنظمة المعلوماتية مستعملين حواسيبهم الخاصة أو حواسيب المدارس التي يدرسون فيها متعدين في ذلك الحدود الجغرافية[7]، ويعود الباعث الأساسي لهذه الفئة إلى الاستمتاع باستخدام هذه التقنية من أجل إثبات مهاراتهم وقدراتهم بكشفهم مواطن الضعف في الأنظمة المعلوماتية دون قصد إلحاق الضرر[8]، وهو ما أدى إلى اختلاف الجهات القانونية في تصنيف هذه الفئة ضمن المجرمين أم لا، باعتبارهم لا يدركون الضرر الذي سيلحق بالغير لقاء

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

تصرفاتهم كما لا يقدّرون مطلقا النتائج المحتملة لأفعالهم غير المشروعة[1]، وهناك من اعتبر تصرفات هذه الفئة من المحظورات التي يعاقب عليها القانون كإجراء ردعي لما قد تؤدي إليه هذه الأفعال من انزلاق أصحابها وانضمامهم إلى فئات محترفي الجرائم المعلوماتية، أو استغلالهم من طرف منظمات أو أفراد سلبيين[2].

2 ــ القراصنة المحترفين Crackers :

وهو نوع يعرف بالمخربين المهنيين، وهم فئة من البالغين الذين تتراوح أعمارهم بين 25 ــ 45 عاما، ومن أبرز سماتهم أنهم يتمتعون بمكانة مرموقة في المجتمع كما يتمتعون بمهارات ومعارف فنية جيدة في مجال المعلوماتية مما يمكنهم من السيطرة الكاملة في بيئة المعالجة الآلية للمعلومات[3].

وتعد هذه الفئة خطيرة مقارنة بالصنف الأول نظرا لما يحدثوه من أضرار بليغة، كما يستمرون في أعمالهم الغير مشروعة ولا يبالون بالأحكام القضائية الصادرة في حقهم، لأن أغلبهم يعتمد في العيش على عائدات جرائمهم إلا أنهم لا يفضلون الأفكار المتطرفة وإنما يسخّرون ذكاءهم في الأفكار التي تدر عليهم الأرباح الشخصية مع عدم مراعاة الأضرار التي تلحق بضحاياهم[4].

الفرع الثاني ــ فئة الحاقدين:

هي صفة تطلق على مجرمي المعلوماتية الذين يقترفون جرائمهم بدافع الثأر والانتقام وعادة ما تكون أفعالهم ضد مرؤوسيهم أو المنشآت التي يعملون بها، حيث يقومون بتصرفات تتصادم والجهود الرامية إلى حماية أنظمة المعلومات التي تستخدمها تلك الجهة سواء كانت شركة أو منظمة أو حتى دولة[5]، وفي هذا الشأن أظهر تقرير صدر في الولايات المتحدة الأمريكية عام 2003م أن 36 بالمائة من الجهات التي شملتها دراسة مسحية أجراها مكتب التحقيق الفيدرالي (FBI) مشاركة مع معهد أمن الحاسوب (Computer Security Institute) أو ما يعرف اختصارا باسم (CSI) يعتبر المستخدمين من

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الداخل خطرا حقيقيا على أنظمة المعلومات[1]، كما سبق لوزارة الدفاع الأمريكية إصدار تقرير في عام 2000م ذكرت فيه أن 87 بالمائة من الهجمات المكتشفة التي شنت على أنظمة المعلومات بالوزارة قام بها أشخاص من داخل الوزارة نفسها[2]، حيث تدور أغلب أنشطتهم في مهاجمة الشبكة الداخلية لأماكن عملهم باستخدام البرامج الضارة لتخريب الأنظمة المعلوماتية أو سرقة المعلومات أو تغييرها أو حذفها، أو فتح ثغرات في أنظمة الحماية التي وضعتها الجهة الضحية لتحصين أنظمة المعلومات فيها بغرض الإتلاف الكلي أو الجزئي للمعطيات المعلوماتية، ورغم أن تصرفاتهم تدور في محور ضيق إلا أن هذا لا يمنع من أن ينجم عنه خسائر جسيمة تضر بالمؤسسات التي يعملون بها[3].

الفرع الثالث ــ فئة المتطرفين:

لقد كان للاختلاف الفكري والأيديولوجي والتعصب المذهبي دور فعالا في بروز هذه الفئة التي تستعمل المعلوماتية كسلاح تشن به الحرب على المخالفين من الطوائف الأخرى بغض النظر عن طبيعة الخلافات سواء كانت دينية أو سياسية أو اقتصادية أو فكرية. وتنشط هذه الفئة على شبكة الانترنت عن طريق نشر وبث واستقبال وإنشاء المواقع والخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري الذي يحرّض على العنف والعنف المضاد أيا كان التيار أو الشخص أو الجماعة التي تتبنى أو تشجع أو تمول كل ما من شأنه توسيع دائرة ترويج مثل هذه الأنشطة[4]. وتسعى هذه الفئة في تحقيق أغراضها الدعائية عن طريق إنشائهم لشبكات إعلامية ومجلات إلكترونية ترصد أنشطتهم وتنشر بياناتهم وتصريحات قادتهم، كما يسخرّون المنتديات والمدونات التي تقوم على تنشيط الحوار حول أفكارهم معتمدين في ذلك أيضا على خدمات البريد الإلكتروني لمجانيته في التواصل مع شركائهم في جميع أنحاء العالم بأسماء تمويهية وعبارات مشفرة[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

فالمجرم المعلوماتي المتطرف تتعدى أهدافه الأغراض الشخصية والمادية إلى فرض أفكاره ومعتقداته على المجتمع لإحداث الفوضى والشتات وزعزعة التماسك الاجتماعي أو الاقتصادي أو الإيديولوجي للأمة.

الفرع الرابع: فئة جواسيس المعلوماتية Cyber-Spies

من أهداف هذه الفئة استخدام الأنظمة المعلوماتية للتجسس على الأعداء والأصدقاء على حد سواء بهدف تفادي شر الغير أوالتفوق عليه، كما لم تعد المعلومات العسكرية هي الهدف الرئيسي بل شملت المعلومات الاقتصادية والتقنية والصناعية وحتى الشخصية في بعض الأحيان[1].

وتتسم هذه الفئة بعدم ارتباطها بغرض محدد، وأغلب من يقومون بهذا العمل هم موظفون في إطار منظم لدى الدول أو الشركات التي يعملون بها، ومن أبرز صور التجسس المعلوماتي؛ استئجار المخابرات الروسية لبعض المختصين في مختلف مجالات المعلوماتية بغرض اختراق الأنظمة المعلوماتية العسكرية للغرب، كما قامت شركتي هيتاشي وميتسوبيشي اليابانيتين بالتجسس على شركة IBM الأمريكية، ولقد أصبحنا نشاهد أو نسمع كل يوم صورا عديدة من صور التجسس الاقتصادي والسياسي والاجتماعي وغيره[2].

الفرع الخامس: فئة مخترقي الأنظمة

تعتمد هذه الفئة على تبادل المعارف فيما بينهم لاكتشاف مواطن الضعف في المنظومة المعلوماتية بغرض استغلالها معتمدين على مجموعة من الأساليب أهمها:

1 ـــ إخفاء الهوية: وهي حيلة تمكن المخترق من الحصول على ملف كلمة الدخول المشفرة الخاصة بالمشرف على شبكة ما، هذا الأخير الذي يقوم بإرسال كلمة السر مشفرة في مختلف مزودات الخدمة* فتظهر هذه الشفرة في بعض المزودات ضمن ملف خاص بكلمة السر ومن ثم تلتقط من طرف المخترق.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ـــ استغلال نقاط الضعف الأمنية المتعلقة بمزودات الويب وأنظمة التشغيل: فأي نظام تشغيل أو مزود ويب لا يخلو من ثغرات قد تعرضه للاختراق إذا اكتشفت من طرف المخترقين الذين بدورهم يستغلونها في عمليات الاختراق ولا يمكن اكتشافهم بسرعة حتى يتمكنوا من الاستفادة منها لفترة طويلة.

3 ـــ استغلال بروتوكول Telnet : كثيرا ما تسمح الثغرات الأمنية في الأنظمة المعلوماتية المختلفة باستخدام تطبيقات تعتمد على بروتوكول Telnet الذي بدوره يسمح بالوصول إلى أجهزة الكومبيوتر عن بعد واختراقها[1].

وتتسم هذه الفئة بأنها غير محددة من حيث العمر فمنهم الصغار والكبار، كما أن نشاطها يعد أقل خطورة من الفئات الأخرى حيث ثبت أن الكثير من الجهات المختصة في إنتاج البرامج تستعين بهم في عمليات فحص وتدقيق مستوى أمن الأنظمة المعلوماتية لديها، أما الكسب المالي فليس من أولوياتهم بقدر متعتهم في إثبات كفاءتهم على اختراق الأنظمة المعلوماتية، وقد بلغ بهم الفضول أن جعلوا من أنفسهم أوصياء على أمن الأنظمة المعلوماتية في مختلف الميادين، أما الخطر الذي قد ينجم عنهم هو احتمال تجنيدهم ضمن هيئات متخصصة في الجريمة الالكترونية حيث ستكون العواقب وخيمة على المجني عليهم بقدر كفاءة الجناة [2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث: المجرم المعلوماتي والهندسة الاجتماعية

إن خداع مستخدمي الحاسوب هو من أكثر الأساليب فعالية التي يهاجم بها المجرم المعلوماتي العنصر البشري وذلك عن طريق ما يسمى بالهندسة الاجتماعية "Social Engineering" ، حيث يبتكر المهاجم حيلا نفسية يخدع بها مستخدمي الحواسيب ليحصل على معلومات تساعده في تحقيق جرائمه[1]، ولقد أفادت الدراسات بأن الهندسة الاجتماعية تعد من أنجح الوسائل استخداما لدى مجرمي المعلومات نظرا لسهولتها مقارنة بالوسائل التقنية الأخرى التي تتطلب الخبرة والجهد الفكري المضني[2].

المطلب الأول: حقيقة الهندسة الاجتماعية

يعتمد المجرم المعلوماتي في الهندسة الاجتماعية على مجموعة من الأساليب، وهي مبينة في الفروع التالية:

الفرع الأول ــ الجانب المادي:

يركز المجرم المعلوماتي في هذا الجانب على مكان الهجوم والبيئة المحاطة به كما يلي:

1 ــ **مكان العمل:** فقد يتظاهر المجرم بأنه أحد عمال النظافة أو الصيانة المتعاقدين ليتمكن من دخول المكاتب بحرية حيث يتاح له جمع كلمات المرور التي عادة ما يلصقها موظفي الحواسيب على شاشاتهم أو ألواح المفاتيح لتفادي نسيانها.

2 ــ **استعمال الهاتف:** بالنظر إلى التركيبة النفسية والاجتماعية للمجتمع تجعل العديد من الأفراد يولون الثقة للغير بسهولة، فيستغل المجرم هذا العنصر كأن يتصل بعمال مراكز الدعم التقني ويستدرجهم بطلب بعض التوضيحات الفنية حيث يحصل على مراده من معلومات وكلمات المرور التي سيستخدمها بعد ذلك في شن هجماته على حواسيب الضحايا كالبنوك، والشركات وغيرها.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

3 ــ **استغلال صناديق المهملات:** هي من أكثر الطرق شعبية لدى المجرمين الذين يستخدمون الهندسة الاجتماعية كما هو الشأن أيضا لدى فرق التحقيق الأمني، فالبحث في المهملات تمكّن المجرم من جمع المعلومات دون لفت أي انتباه، فقد يحصل على كلمات المرور أو دليل هواتف الشركة، أو نسخ من مواعيد الاجتماعات، أو نسخ من فواتير الشراء ..الخ، وهي معلومات تفيد المجرم في التظاهر بأنه أحد المشاركين فيخدع أمناء الإدارة بمعلوماته التي وقعت حقا بالمؤسسة وبالتالي يحصل منهم على ما يريد من معلومات مفيدة في شن جريمته، كأن يطلب منهم أن يرسلوا له نسخة من محضر الاجتماع التفصيلي والذي قد يحتوي على بيانات هامة.

4 ــ **استعمال الإنترنت:** هناك الكثير من البرمجيات الوظيفية التي تتطلب كلمات المرور، وتفاديا للنسيان يعتمد الكثير من المستخدمين كلمة مرور واحدة لجميع البرامج، وهي ثغرة يستغلها المجرم المعلوماتي حيث يعرض خدمات مجانية على شبكة الانترنت؛ كتنزيل البرامج، وإمكانية تحميل الكتب الرقمية أو الألعاب ويشترط قبل التحميل أن يسجل المستفيد دخوله بكلمة مرور، وعادة ما يقع من يستخدم كلمة المرور الموحدة في فخ المجرم الذي بدوره سيستخدمها في الحصول على مبتغاه من المعلومات المخزنة لدى الضحية[1].

الفرع الثاني ــ الجانب النفسي:

إن كسب ثقة الضحية تجاه المجرم عن طريق خلق أجواء نفسية مناسبة كإيهامه بأنه شخصية موثوق فيها ويتمتع بصلاحيات معرفة المعلومات الحساسة للهيئة المستهدفة[2] مستخدما في ذلك عدة أساليب أبرزها:

1 ــ أسلوب الإقناع: هو من أهم أساليب الهندسة الاجتماعية التي يستعملها المجرم المعلوماتي في خداع الضحية معتمدا في ذلك على جوانب عدة أهمها:

أ ــ طرق الإقناع: فحسب ما توصل إليه علم النفس الاجتماعي، أنه لإقناع أي شخص في تنفيذ شيء ما لابد من سلوك إما الطريقة المباشرة في الإقناع وإما الطريقة غير المباشرة؛ كأن يتذرع

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المجرم بالحجج المنطقية والبراهين لتحفيز المتلقي ـــ الضحية ـــ على التفكير المنطقي من أجل الوصول إلى نتيجة يهدف المهاجم في جر الضحية إليها وهذه هي الطريقة المباشرة.

أما الطريقة غير المباشرة يعتمد فيها المهاجم على الإيحاءات النفسية وتخطي المنطق متحاشيا إثارة قدرة التفكير المنطقي لدى الضحية من أجل خداعه بقبول مبررات المهاجم بدون تحليل أو تفكير جدي؛ كأن يعتمد في بداية لقائه بالضحية إلى استعمال عبارات يتأثر بها المستهدف نفسيا كبث مشاعر الخوف، أو مشاعر الحماس في نفسه فتتشكل لديه موجة من المشاعر التي تعمل على تشويش تفكيره وبالتالي تضعف قدراته على التحليل المنطقي مما يصعب عليه مواجهة حجج المهاجم وإن كانت ضعيفة، ومن أمثلة الأساليب غير المباشرة في الإقناع ما يلي[1]:

ـــ أسلوب الإغراء النفسي: فقد أثبتت دراسات كثيرة أجريت في مجال علم النفس الاجتماعي أن رغبة الأشخاص لامتلاك الأشياء تزداد كلما أحسوا بندرتها أو خصوصيتها، وهو سلوك يستغله المجرم المعلوماتي كأن يعرض في موقعه الالكتروني إمكانية التحميل المجاني لبرامج نادرة جدا، ثم يعلن بأن هذا العرض سار لمدة محدودة فقط، ويشترط في عملية التحميل إدخال اسم المستخدمUser Name وكلمة المرور Password وقد تكون نفسها المعلومات التي يستخدمها الضحية في تطبيقاته الخاصة كالبريد الإلكتروني، أو قاعدة بيانات المؤسسة التي يعمل بها.

ـــ انتحال أوجه التشابه مع شخصية الضحية: عادة ما تميل النفس البشرية إلى من يتطابق معها في العرق أو اللون أو الاهتمامات والطباع، وهذا الميول يولد الإحساس بالطمأنينة تجاه الطرف الآخر مما يؤدي إلى التعطل اللا إرادي في قدرات التحليل والتفكير المنطقي.

وهي نقطة ضعف أيضا يستغلها المهاجم؛ حيث يقوم بجمع معلومات شخصية تخص الضحية كمكان ميلاده والهويات التي يمارسها ونحوها، ثم يشرع في محاورة المستهدف ويوهمه بأنه ولد في نفس التاريخ والمدينة أيضا، أو أنه يمارس الهوايات نفسها فتنبني علاقة لا أصل لها نتيجة استرخاء المستهدف ذهنيا، وبعدها يبدأ المهاجم باستدراج المستهدف من أجل الحصول على ما يريده من معلومات.

---

(1) الإحالات في النسخة المطبوعة

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ رد الجميل: تتميز النفس البشرية السوية برغبة الإحسان إلى من أحسن إليها، ومن باب من أسدى إليك معروفا فإنك ملزم أدبيا بمقابلة ذلك المعروف بمثله أو أحسن منه، وهي ذريعة يستغلها المهاجم كتقديمه خدمة في صورة حل مشكلة تقنية أو استرجاع ملفات ضائعة حذفت على سبيل الخطأ، فيشعر المستهدف أنه مدين لمن أخرجه من مأزق محتم وبذلك يفتح الطريق للمهاجم بإعطائه بعض المعلومات حتى وإن كانت سرية، كما قد يسمح له باستخدام الجهاز الذي يعمل عليه للإطلاع على الانترنت مثلا وهو ما يمكنه من زرع بعض البرامج الخبيثة التي تتيح له اختراق الشبكة الخاصة بالمؤسسة عن بعد.

2 ـــ أسلوب انتحال الشخصية:

وهو أسلوب يسهل استعماله في الهيئات والتجمعات الكبيرة التي لا يعرف أفرادها بعضهم البعض، ومن الشخصيات التي يكثر انتحالها في مجال الهندسة الاجتماعية؛ شخصية فني صيانة معدات الحواسيب والشبكات، أو شخصية المسؤول، أو عامل النظافة، أو أمين المكتب، أو إطار سام مكلف من قبل الإدارة العليا لهيئة ما، فقد يتصل مجرم المعلومات بأفراد مركز تقديم الدعم التقني بالمؤسسة ـــ الضحية ـــ منتحلا شخصية أمين مكتب المدير، مدعيا أن المدير كلفه بأن يطلب منهم كلمة مرور جديدة لبريده الالكتروني لنسيانه كلمة المرور السابقة، كما يوهمهم بأن الوضع لا يقبل الانتظار لأنه مرتبط باجتماع هام يحضره المدير في اللحظات القليلة القادمة وهو بحاجة ماسة إلى مراجعة الوثائق الهامة المرسلة إليه ذات العلاقة بالاجتماع، وبالنظر إلى أهمية هذه الحجج فإن أفراد مركز تقديم الدعم الفني قد يصدرون كلمة مرور جديدة ويعطونها لمنتحل الشخصية وبذلك يقتحم البريد الخاص لمدير المؤسسة.

3 ـــ أسلوب المداهنة:

المداهنة صفة يحبذها الكثير من العاملين تحت سلطة ما، وهي من الأساليب التي يستغلها المهاجم حين ينتحل شخصية معينة فإنه يعلم يقينا أن كثيرا من موظفي الهيئة المستهدفة سيسعون جاهدين لخلق صورة حسنة عن أنفسهم لدى رؤسائهم، وبالتالي فإنهم لا يترددون في تقديم المعلومات التي يطلبها منتحل الشخصية باعتباره ذو سلطة أو ذو صلة بصاحب السلطة.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

4 ــ أسلوب المسايرة:

وهو أسلوب يتصف بالحيطة ومسايرة ما اعتاد الناس عليه كي لا يلفت النظر، كأن يقدم المجرم نفسه للمستهدف على أنه مكلف من إدارة الشبكة الرئيسية في مهمة لتقديم الدعم الفني للمؤسسات، ويوهم المستهدف أن مهمته هي تحديث نسخة جديدة من برنامج ما قد تم تثبيته في أجهزة المؤسسات التي تستفيد من هذه الشبكة مما يولد شعورا خفيا لدى المستهدف بعدم الرفض نظرا للمصلحة التي سيحدثها منتحل الشخصية، وهو ما يتيح للمهاجم فرصة تثبيت برامج خبيثة في جهاز المستهدف.

5 ــ أسلوب الهندسة الاجتماعية العكسي:

يعد هذا الأسلوب من أكثر الطرق استعمالا لدى المجرم المعلوماتي، وذلك باختلاقه لوضع ما يتيح له أن يظهر في صورة الكفاءة العالية فيتوجه إليه المستهدفون طالبين المساعدة وتلقي المعلومات؛ كأن يخرب المهاجم موضعا يتعذر الوصول إليه بسهولة من شبكة المعلومات للمؤسسة المستهدفة، فتنقطع الخدمة جزئيا أو كليا وهي مرحلة افتعال الموقف، ثم في المرحلة الثانية يقدم نفسه على أنه أحد تقنيي فريق الدعم الفني وباستطاعته حل المشكلة، وتأتي المرحلة الثالثة بتقديمه للمساعدة التي ستبهر الموظفين الذين سيتوجهون إليه بالأسئلة عما إذا كانوا سيفقدون الوثائق التي يعملون عليها لحظة انقطاع الشبكة، وهل كلمات المرور التي لم يتم إغلاقها لابد من استبدالها..الخ، فيسمحون له بحرية التحقق منها وبذلك يكون قد نجح في اختراق نظام معلومات الشركة دون أن يشعر أحدا.[1]

وما نخلص إليه أن الهندسة الاجتماعية هي من أنجع الأساليب التي يستغلها مجرمي المعلومات في مهاجمة المنظومة المعلوماتية، ولذلك يجب أن تكون على رأس قائمة المعنيين بحماية المعلومات، خاصة وأنها صفة ذميمة ينهى عنها الشرع الإسلامي.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الرابع:

المجتمع المعلوماتي ومؤشراته

المبحث الأول: مفهوم المجتمع المعلوماتي.

المبحث الثاني: المؤشرات الإحصائية للمجتمع المعلوماتي

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

تمهيد:

لقد عرف المجتمع المعلوماتي مصطلحات عديدة تتقاطع في تعريفاتها مع ثورة تكنولوجيا المعلومات ومن بينها أنه؛ مجتمع ما بعد الصناعي (post-industrial society) ، ومجتمع ما بعد الحداثة (postmodern society) ، ومجتمع المعرفة (knowledge society)، والمجتمع الرقمي (digital society)، ومجتمع الشبكات (network society) .. [1]، خاصة وأن تكنولوجيا المعلومات والاتصال أصبحت من بين أهم المقومات الأساسية للدول حيث تقاس قوتها بمدى تحكمها في التكنولوجيا وإنتاجها للمعرفة وهو ما أدى إلى اعتماد الدول المتقدمة توجها جديدا في مجال الاقتصاد يعتمد على التوظيف الفعال للمعلومة والمعرفة (Knowledge Economy) من أجل تحقيق القيمة المضافة وتنمية الناتج المحلي الخام. [2]

ولقد صدر في هذا الشأن تقرير للاتحاد الدولي يشير إلى "أن المجتمع على المستوى العالمي قد بلغ في نهاية سنة 2008م إلى مستويات معتبرة من حيث استعمال وتبني تكنولوجيا الاتصال الحديثة، حيث ارتبط ربع سكان العالم بشبكة الانترنت كما يملك الأفراد حوالي 04 بليون هاتف نقال، وتم استغلال 1.3 بليون خط هاتفي ثابت" وهي مؤشرات تبين مدى حجم المجتمع المعلوماتي الذي يستدعي دراسته والتعرف عليه من خلال المباحث التالية [3].

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول:

مفهوم المجتمع المعلوماتي (Information Society) وخصائصه

المطلب الأول: التعريف الاصطلاحي للمجتمع المعلوماتي

يعود ظهور مصطلح المجتمع المعلوماتي إلى النصف الثاني من القرن العشرين بعد القفزة الهائلة التي عرفها العالم في مجال تكنولوجيا المعلومات، حيث شهد هذا المصطلح تعريفات عديدة وذلك وفق وجهات النظر المتباينة والخلفيات التي انطلقت منها، ومن أبرزها ما يلي:

المجتمع المعلوماتي هو: "المجتمع الذي يعتمد في تطوره بصورة أساسية على المعلومات وشبكات الاتصال والحواسيب" أي المجتمع الذي يعتمد على "التقنية الفكرية"؛ "تلك التي تضم سلعا وخدمات جديدة مع التزايد المستمر في القوة العاملة المعلوماتية" وهو تعريف يربط التطور الإنساني من حيث الفكر والعقل بالحواسيب والاتصال والذكاء الاصطناعي (Expert System) [1].

ويعرّف بأنه: المجتمع الذي اعتمد أساسا على تقنيات المعلومات والتكنولوجيا الحديثة، نظرا لضرورتها الحتمية لكل فرد وتعاظم دورها في كافة المجالات الاقتصادية والسياسية والعلمية والاجتماعية، وهذا وفق المتغيرات التكنولوجية الكبيرة الحاصلة بسبب ما يسمى "بالثورة المعلوماتية أو الانفجار المعلوماتي" [2].

وجاء في تعريف آخر: "هو مجتمع يستطيع فيه كل فرد استحداث المعلومات والمعارف والنفاذ إليها واستخدامها و تقاسمها بحيث يمكن للأفراد و المجتمعات و الشعوب تسخير كامل إمكاناتهم في النهوض بتنميتهم المستدامة وفي تحسين نوعية حياتهم" [3]

كما يعرّف أيضا المجتمع المعلوماتي: بأنه مصطلح للمجتمع الذي أصبحت أهم مقوماته الاقتصادية والعلمية تقوم على أساس الإنتاج والتوزيع والتحكم في المعلومات. و يمكن مقارنة المجتمع المعلوماتي مع المجتمعات الصناعية والزراعية؛ بأن وسائل الإنتاج لدى المجتمع المعلوماتي تتمثل في

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الحواسيب والاتصالات، بينما المجتمعات الأخرى تعتمد في وسائلها على آلات التصنيع والمحاريث[1].

و جاء في تعريف آخر بأنه: المجتمع الذي يقوم أساسا على نشر المعرفة و إنتاجها و توظيفها بكفاءة في جميع مجالات النشاط المجتمعي من الاقتصاد، و المجتمع المدني، و السياسة، و الحياة الخاصة وصولا للارتقاء بالحالة الإنسانية باطراد أي إقامة التنمية الإنسانية[2] .

و يعرّف بأنه: المجتمع الذي يعتمد في تطوره بصورة أساسية على المعلومات وشبكات الاتصال والحواسيب أي أنه يعتمد على ما يسميه البعض " بالتقنية الفكرية "ـــ تلك التي تضم سلعًا وخدمات جديدة مع التزايد المستمر في القوة العاملة المعلوماتية ـــ بمعنى تعظيم شأن الفكر والعقل الإنساني بالحواسيب والاتصال والذكاء الاصطناعي (expert system) [3].

و يعرّف بأنه؛ المجتمع الذي أعتمد أساسا على المعلومات وتقنيات المعلومات والتكنولوجيا الحديثة، و أصبحت المعلومات فيه لازمة لكل فرد وتعاظم دورها في كافة المجالات الاقتصادية والسياسية والعلمية والاجتماعية[4].

و من خلال هذه التعريفات يتضح أن السمة الأساسية التي تميز هذه المرحلة الجديدة أو المجتمع الحديث، هي تعاظم قيمة المعلومات في شتى الميادين واستخدامها بكثافة كوجه للحياة الاقتصادية، والاجتماعية، والثقافية والسياسية، و كمورد استثماري، وكسلعة إستراتيجية، وكخدمة، وكمصدر للدخل القومي، وكمجال للقوى العاملة[5].

المطلب الثاني: أسباب نشوء مجتمع المعلومات

هناك مجموعة من الأسباب ساهمت في ظهور وتطور مجتمع المعلومات وهي كالآتي: [6]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أولا ــ المراحل التاريخية للتطور الاقتصادي: فالمراحل الطويلة التي شهدتها بُنا الاقتصاد العالمي من تغيرات جذرية ابتداء من العصر المشاع الذي كان يعتمد فيه الإنسان على ما تدره الطبيعة من خيرات معتمدا في قوى إنتاجه على الطاقات الطبيعية و الجهد العضلي، مرورا بالعصر الصناعي الذي اعتمد الطاقات المولدة، ووصولا إلى عصر المعلوماتية الذي تحتل فيه المعلومات والمعرفة الأهمية القصوى و يعتمد عليها مجتمع المعلومات بصورة أساسية في اقتصادياته.

ثانيا ــ الثورة التكنولوجية : عرف النصف الثاني من القرن العشرين تطورات سريعة في المجال التكنولوجي خصوصا بعد اختراع الحاسوب وإقحامه في كافة مجالات الحياة، وكنتيجة لذلك ساهمت تكنولوجيا المعلومات والاتصالات في التأثير الإيجابي على النمو الاقتصادي نظرا لما تتميز به من مرونة في تطبيقها الواسع في مختلف المجالات، وكنتيجة لذلك زاد الطلب عليها باستمرار من أجل الاستفادة من إمكانياتها وخصائصها فضلا عن أن تكاليفها تتجه نحو الانخفاض بصورة واضحة.

ثالثا ــ الظاهرة المعلوماتية: يشير مصطلح الظاهرة المعلوماتية إلى الاتساع السريع في رقعة المجال الذي أحدثته المعلومات لتشمل كافة مجالات النشاط الإنساني، حيث أصبح للمعلومات سوق كبير لا يقل أهمية عن أسواق مواد الطاقة والمعادن النفيسة، وأدى التزايد المستمر في المعلومات وظهور تخصصات جديدة في المعارف البشرية ونمو قوى الإنتاج والاستهلاك إلى تراكم الرصيد المعلوماتي الذي بدوره شكل ما يعرف بظاهرة الانفجار المعلوماتي، الذي تعود أسبابه إلى:

- الكم الهائل والمتزايد في المطبوعات والمنشورات المتنوعة.
- صعوبة الاختيار النوعي للمواد المطلوبة ضمن وفرة الكم الهائل منها.
- انهيار الحدود بين الموضوعات وتداخل التخصصات العلمية.
- فشل الأساليب والوسائل التقليدية في الضبط والسيطرة على تنظيم هذه المعلومات المتراكمة يوما بعد يوم[1].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثالث: خصائص مجتمع المعلومات:

يتميز مجتمع المعلومات عن المجتمعات التقليدية بعدة خصائص أهمها:

أولا ــ اعتماد المعلومات كمورد اقتصادي :

فمعظم المؤسسات العالمية المعاصرة تعتمد في تحسين وضعيتها التنافسية على استخدام المعلومات لتدعيم أنشطة التجديد والابتكار، وذلك عن طريق تطوير عروضها التي تقدمها من خلال ابتكار مواصفات جديدة لمنتجاتها التقليدية أو العمل على خلق منتجات لم تعرض من قبل، ولقد برز في هذا السياق شركات المعلومات التي تسهم بكميات هائلة في القيمة التي تعمل على تحسين الاقتصاد الكلي للدول.

ثانيا ــ الاستخدام العام للمعلومات :

ففي وقتنا الراهن أصبحت المعلومات جزء من حياة الناس، حيث يستخدمونها بكثافة في أنشطتهم كمستهلكين ومتعلمين، ويستعملونها كمواطنين لممارسة واجباتهم وحقوقهم المدنية، وبذلك تكون المعلومات عنصر لا غنى عنه في الحياة اليومية للفرد والمجتمع.

ثالثا ــ بروز قطاع المعلومات لأهميته في الاقتصاد القومي :

يعد بروز قطاع المعلومات حتمية فرضت نفسها في عصر العولمة ليصبح القطاع الرابع في النشاط الاقتصادي القومي بجانب قطاع الزراعة، والصناعة، والخدمات، كما أصبح إنتاج المعلومات وتجهيزها وتوزيعها من أهم اقتصاديات العديد من الدول، وبذلك تغير مفهوم اقتصاد الصناعات إلى اقتصاد المعلومات ومن اقتصاد محلي إلى اقتصاد لا يعرف الحدود، ومن إنتاج السلع والخدمات إلى إنتاج المعلومات. كما عرفت القوى العاملة في الأنشطة المعلوماتية تزايدا مستمرا يفوق إجمالي القوى العاملة في المجالات الاقتصادية التقليدية خاصة في قطاعات التعليم والبحوث والتنمية والاتصالات والحواسيب والأجهزة الذكية وخدمات المعلوماتية.[1]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني: المؤشرات الإحصائية للمجتمع المعلوماتي

إن المعرفة الإحصائية للمجتمع المعلوماتي على المستوى العالمي يعطي للبحث محل الدراسة مصداقية هامة؛ فعرض المؤشرات الإحصائية يسمح لنا بأن نتصور حجم المخاطر الناجمة عن الجرائم الإلكترونية، وذلك بالنظر إلى ما تعكسه هذه الإحصاءات من مدى اعتماد المجتمعات المعاصرة على التكنولوجيا الحديثة في تحقيق المصالح العامة والخاصة.

ونظرا لأهمية هذه الإحصاءات فقد سخرّت مواقع إلكترونية متخصصة تعمل باستمرار على ترجمة أنشطة المجتمع المعلوماتي إلى أرقام وبيانات تتعلق بكل ما يتدفق من شبكة الانترنت العالمية، وهي إحصاءات في غاية الأهمية لكونها تغذي التقارير والأبحاث والدراسات الإحصائية بما تتطلبه من أرقام وبيانات فتزيد من قيمتها العلمية. والمطالب التالية توضح أهم المؤشرات المتعلقة بالمجتمع المعلوماتي في نهاية سنة 2012م[1].

المطلب الأول: تعداد مستخدمي الانترنيت ونطاقاتها:

1 ــ عدد مستخدمي الانترنت[2]:

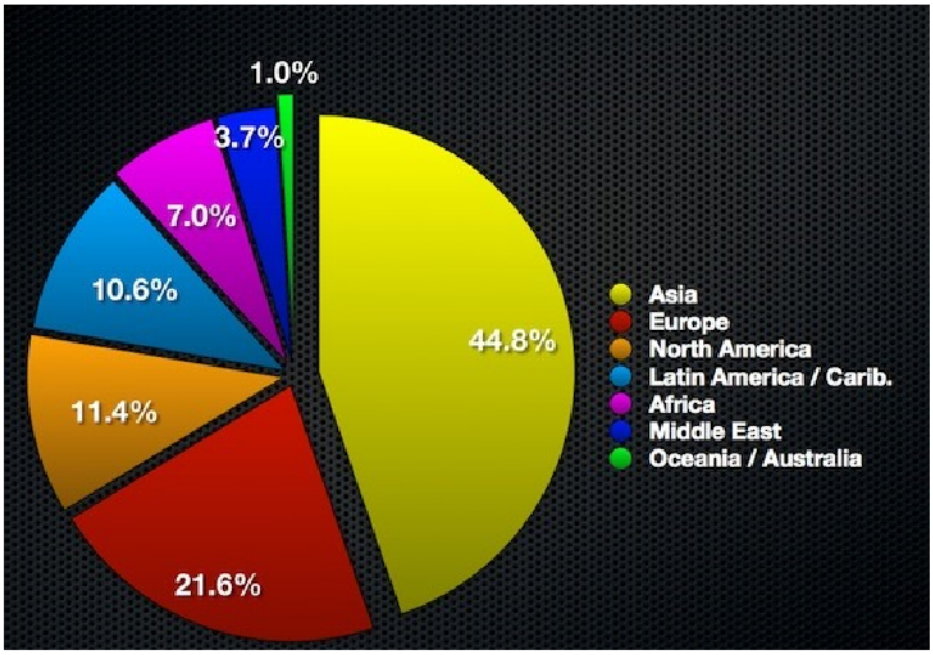
- 2.4 مليار مستخدم للانترنت في العالم.
- 1.1 مليار مستخدم للانترنت في آسيا.
- 274 مليون مستخدم للانترنت في أمريكا الشمالية.
- 255 مليون مستخدم للانترنت في أمريكا اللاتينية.
- 167 مليون مستخدم للانترنت في أفريقيا.
- 90 مليون مستخدم للانترنت في الشرق الأوسط.
- 24 مليون مستخدم للانترنت في استراليا.
- 565 مليون مستخدم للانترنت في الصين وحدها.
- 42 % نسبة انتشار الانترنت في الصين مقارنة بمجموع مستخدمي الانترنت في العالم.

---

(1) الإحالات في النسخة المطبوعة.

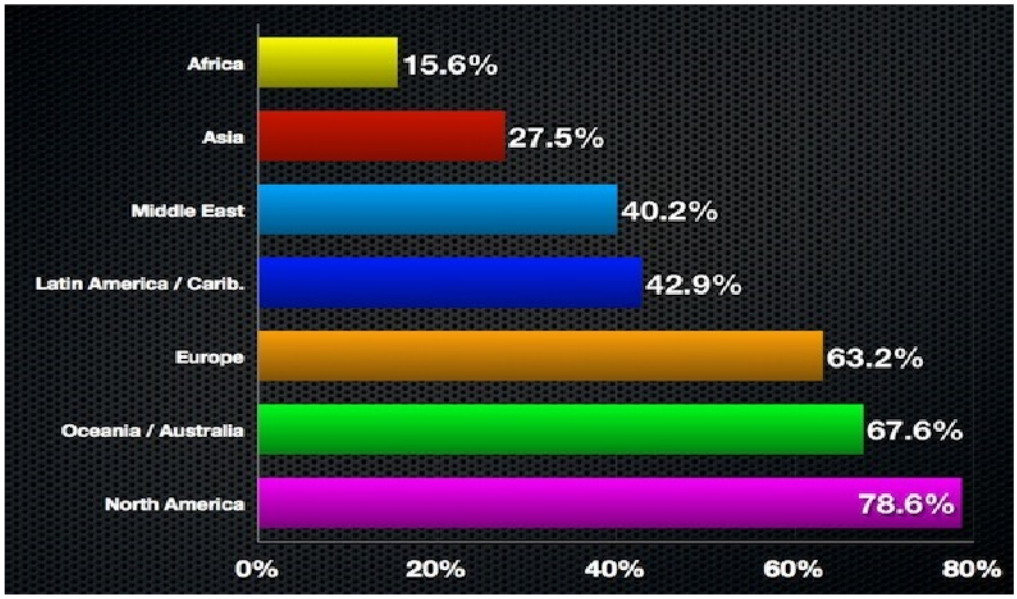
(2) الإحالات في النسخة المطبوعة.

...../...



شكل رقم (04)، رسم بياني يمثل نسبة انتشار الانترنت بحسب المنطقة[1]

والرسم البياني التالي يبين نسب الاختراقات الإلكترونية الحاصلة حسب المنطقة خلال سنة 2012 :



الشكل (05) رسم بياني يبين نسب الاختراقات الإلكترونية الحاصلة حسب المنطقة خلال سنة 2012[2]

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ــ النطاقات النظامية Domain Name System **

- 246 مليون نطاق مسجل.
- 104.5 مليون نطاق خاصة بالدول.
- 100 مليون نطاق دوت كوم في عام 2012
- 14 مليون نطاق دوت نت في عام 2012
- 9.7 مليون نطاق دوت org في عام 2012
- 2.4 مليون دولار قيمة نطاق Investing وهو الرقم الأعلى في عام 2012

المطلب الثاني: تعداد مستعملي تطبيقات الشبكات[1].

1 ــ البريد الإلكتروني*:

- بلغ عدد مستخدمي البريد الإلكتروني في العالم 2.2 مليار مستخدم.
- كما بلغ حجم تدفق بيانات البريد الإلكتروني 144 مليار تدفق.
- وبلغت تطبيقات ومواقع خدمة البريد الإلكتروني مليار تطبيق أو موقع.
- 35 % منها كان نصيب تطبيقات البريد الإلكتروني الخاص بأجهزة الآيفون.
- بلغ عدد مستخدمي بريد الجيميل (Gmail)** 425 مليون مستخدم مما يجعله البريد الأول استعمالا في العالم.
- 68.8 % من تدفق بيانات البريد الإلكتروني جاءت من رسائل السبام*** (Spam)

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

- أكثر من 50% من رسائل السبام في عام 2012 تتعلق بالمستحضرات الصيدلانية.
- 22 % من البريد المخترق تم من خلال الاصطياد الإلكتروني.*

4 ــ الشبكات الإجتماعية

- مليار مشارك في الفيس بوك facebook.
- 47 % من مستخدمي الفيس بوك من النساء.
- 40 سنة متوسط سن مستخدمي الفيس بوك.
- 2.7 مليون ضغطة لزر الإعجاب يوميا في الفيس بوك.
- 24 % من أكثر 10 ألاف موقع زيارة توفر التكامل مع الفيس بوك.
- 200 مليون مستخدم نشط شهريا في تويتر.
- 175 مليون تغريده يتم نشرها يوميا في تويتر.
- 37 سنة متوسط سن مستخدمي تويتر.
- معدل التغريدات للمستخدم الواحد هو 307 تغريده.
- معدل المتابعين للمستخدم الواحد هو 51 متابع.
- 163 مليار تغريده تم نشرها من إنطلاقة تويتر.
- 200 مليون مستخدم في شبكة لينكدان.
- 44 سنة معدل سن مستخدمي لينكدان.
- 135 مليون مستخدم نشط في قوقل بلس (Google+).
- 5 مليار استخدام لزر +1 الخاص بقوقل بلس في اليوم الواحد.

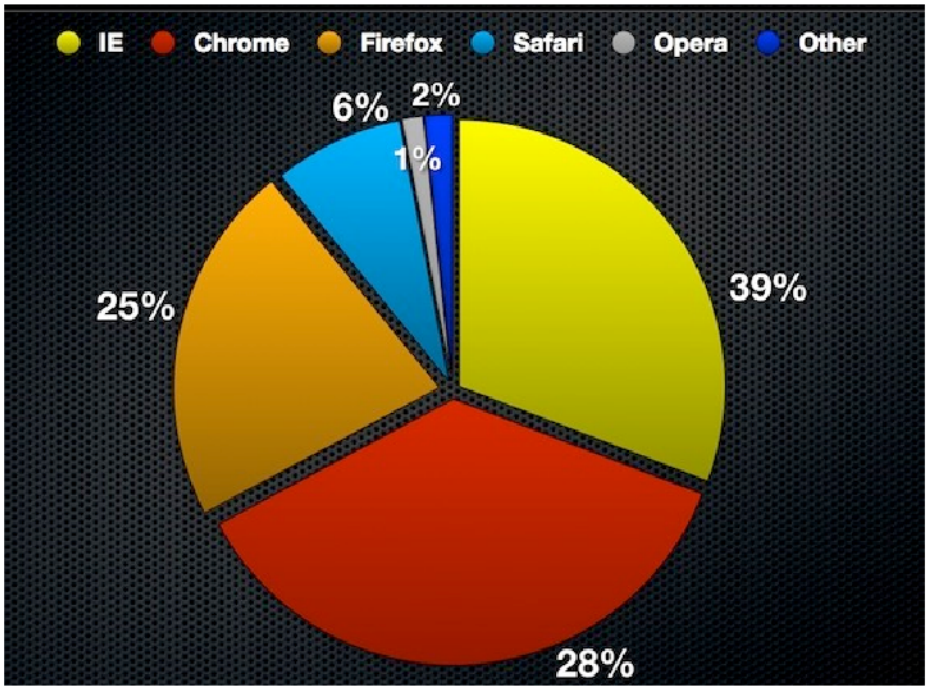
5 ــ المتصفحات Browsers *

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

بلغت حصة المتصفحات الرئيسية حتى ديسمبر عام 2012 كما يلي:



شكل (06) رسم بياني يبين حصة المتصفحات الرئيسية بالنسب المئوية حتى ديسمبر عام 2012 (1)

6 ــ استعمال محركات البحث*:

- 1.2 تريليون بحث في قوقل google عام 2012.
- بلغت حصة قوقل في سوق محركات البحث 67 %.

7 ــ مشتركي الهواتف:

- 1.1 مليار مشترك من خلال الهواتف الذكية.
- 6.5 مليار مشترك في خدمة الهواتف.
- 5 مليار عدد مستخدمي الهواتف.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

- 465 مليون هاتف اندرويد[1] تم بيعه في 2012 .
- 31 % من مستخدمي الانترنت في أمريكا يستخدمون أجهزة الألواح الذكية، و جهاز القارئ الإلكتروني.*
- 13 % من تدفق البيانات في الانترنت من الهواتف.
- 5 مليار مشترك في خدمة البرودباند Broadband ** الخاصة بالهواتف.
- 1.3 اكسابايت *** كمية تدفق البيانات المتداولة شهريا من خلال الهواتف.
- 59 % من البيانات التي تم تداولها من خلال الهواتف هي مقاطع الفيديو.
- معدل استهلاك الهواتف الذكية هو 500 ميقا بايت شهريا.

8 ــ استعمال خدمات الفيديو:

- 14 مليون مستخدم في خدمة فيميو Vimeo **** .
- حجم مقاطع الفيديو التي تم تشغيلها من خلال خدمة فيميو في عام 2012 هو200 بيتابايت *****
- 150 مليون زائر غير مكرر لمواقع فيديو قوقل.
- 2.5 مليون ساعة تم رفعها لليوتوب Youtube متعلقة بالأخبار.

كما بلغت عدد المشاهدات المباشرة للفيديو باستعمال الانترنت:

- 4 مليارات ساعة في مشاهدة مقاطع اليوتوب شهريا.
- 60 مليون مشاهد شهريا لخدمة Ustream .

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

- 16 مليون مشاهدة هي المشاهدة الأعلى خلال 24 ساعة في خدمة Ustream*

- 181 مليون مشاهد غير مكررين لمقاطع الفيديو من خلال الانترنت في أمريكا فقط.

9 ــ الإطلاع على الصور واستعمالها:

- 7 بيتابايت من الصور يتم رفعها في الفيس بوك شهريا.

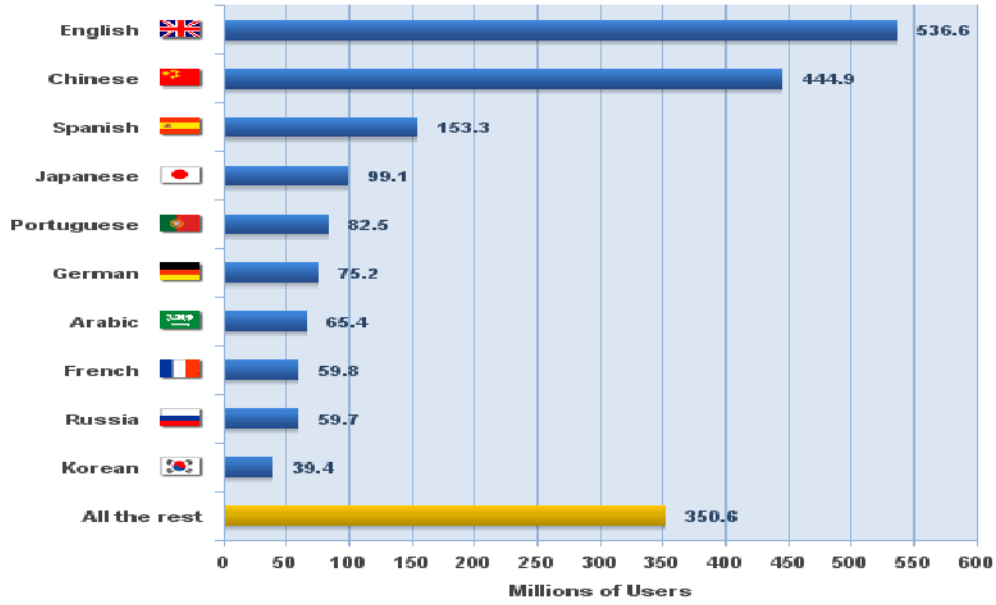
- 300 مليون صورة يتم رفعها للفيس بوك يوميا.

- 5 مليارات صورة تم رفعها لخدمة موقع انستقرام المخصص للصور الحرة.

المطلب الثالث : مؤشرات المجتمع المعلوماتي في العالم العربي

الفرع الأول: المؤشرات الرقمية

قامت دراسة إحصائية أجريت سنة 2010م[1] بتصنيف أكثر اللغات العالمية استعمالا في الانترنت، وقد تم ترتيب اللغة العربية في المرتبة السابعة باعتبارها من أكثر اللغات استعمالا للانترنت بعد اللغة الانجليزية، واللغة الصينية، والإسبانية، واليابانية، والبرتغالية، والألمانية، ونستنتج من ذلك مدى أهمية حجم المجتمع المعلوماتي العربي بنظيره في العا لم وهو ما يبينه الشكل التالي:



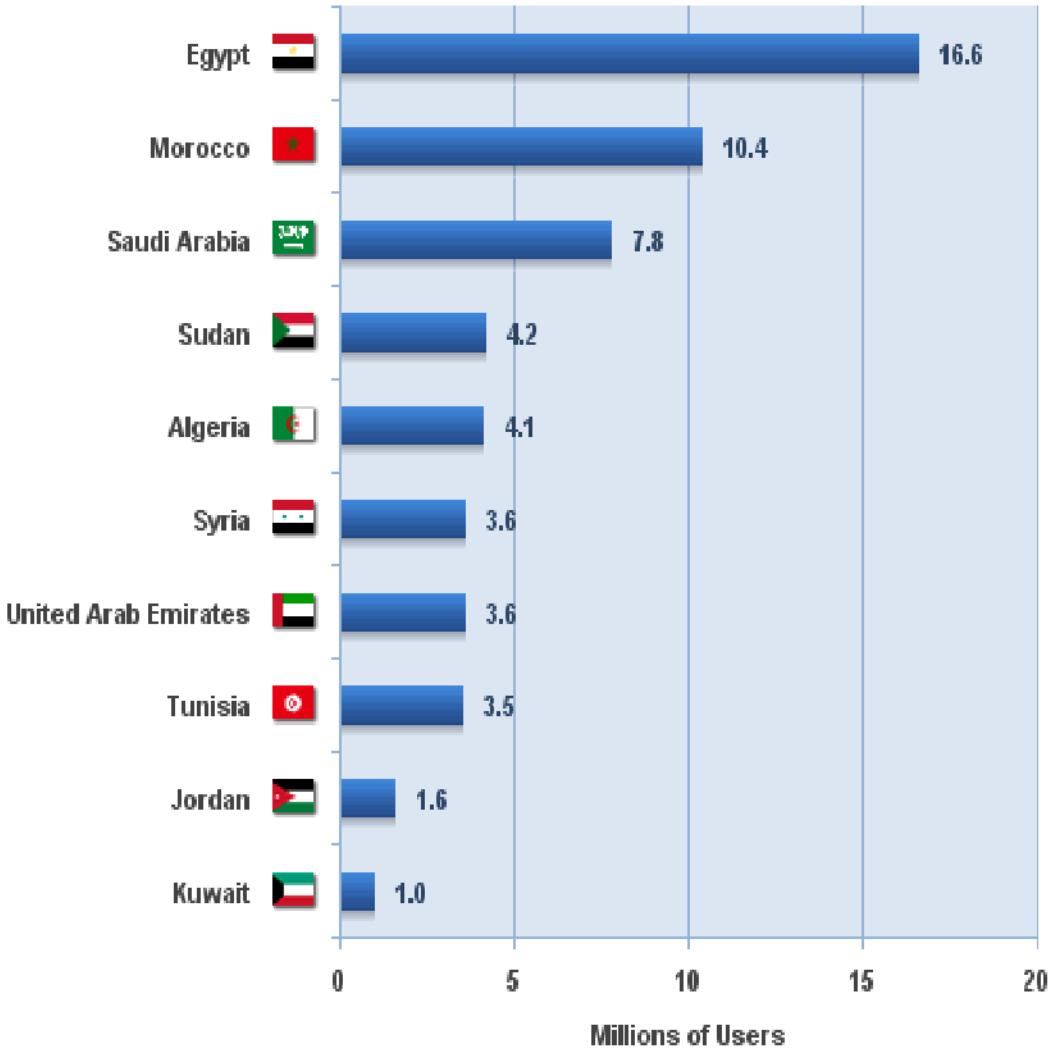
الشكل رقم:(07): يبين أكثر اللغات استعمالا على الانترنت[2] (الأرقام ضرب مليون مستعمل)

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

أما الشكل التالي يبين لنا ترتيب الدول العشر الناطقة باللغة العربية الأكثر استعمالا للانترنت، وذلك من خلال دراسة إحصائية أجريت سنة 2009[1]، حيث يظهر من خلالها أن الجزائر تحتل المرتبة الخامسة في التصنيف:



الشكل رقم(08): يبين الدول العشر المصنفة الأكثر استعمالا للانترنت[2] بالنسبة للدول الناطقة باللغة العربية (الأرقام ضرب مليون مستعمل).

أما مستعملي الانترنت على مستوى الدول الناطقة باللغة العربية يمكن حصرها في الجدول الإحصائي التالي[3]:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

الجدول رقم(01): يبين مستعملي الانترنت في الدول الناطقة باللغة العربية

(تقدير 31 ديسمبر 2011)

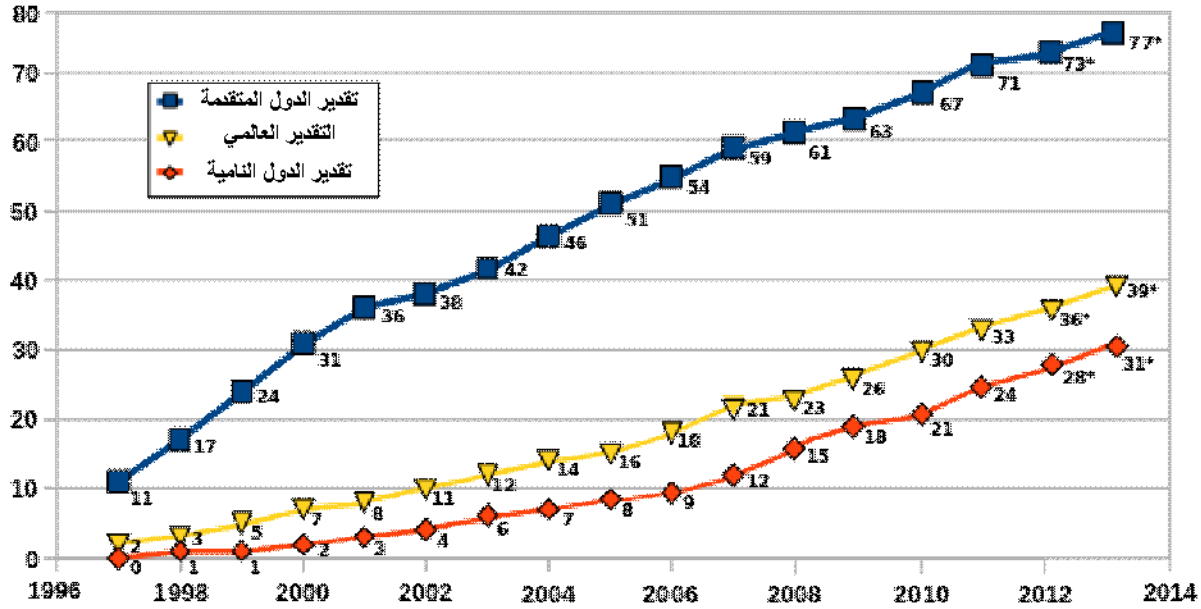
الدول	التعداد السكاني	مستخدمو الانترنت	مستخدمو الفيس بوك[1]
الجزائر	34,994,937	4,700,000	3,432,800
البحرين	1,214,705	694,009	351,680
جزر القمر	794,683	37,472	13,460
جيبوتي	757,074	61,320	43,320
مصر	82,079,636	21,691,776	10,740,440
العراق	30,399,572	1,303,760	1,655,640
الأردن	6,508,271	1,987,400	2,194,880
الكويت	2,595,628	1,100,000	970,640
لبنان	4,143,101	1,367,220	1,415,740
ليبيا	6,597,960	391,880	514,160
موريتانيا	3,281,634	100,333	85,440
المغرب	31,968,361	15,656,192	4,318,500
عمان	3,027,959	1,741,804	471,760
قطر	1,759,227	1,231,567	550,400
السعودية	26,131,703	11,400,000	5,373,820
الصومال	9,925,640	106,000	81,940
السودان	36,787,012	4,200,000	غير معروف
سوريا	22,517,750	4,469,000	غير معروف
تونس	10,629,186	3,856,984	2,984,940
الإمارات	8,264,070	5,859,118	3,217,100
فلسطين	2,568,555	1,512,273	910,600
اليمن	24,133,492	2,606,698	526,280
المجموع	**359,340,646**	**86,077,806**	**39,853,540**

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والملاحظ من خلال الجدول أن الجزائر تتصدر المرتبة الخامسة بين الدول الناطقة باللغة العربية من حيث استعمال الانترنت، كما أن الأرقام المذكورة في الجدول تبين مدى ضخامة المجتمع المعلوماتي العربي الذي يشهد تزايدا مطردا مع التقدم في الزمن، وهو ما يترجمه الشكل البياني التالي:



شكل رقم (09): يبين عدد مستخدمي الانترنت لكل مائة ساكن عبر السنوات(1)

يتضح من خلال الشكل البياني التزايد المستمر في عدد مستخدمي الانترنت لكل مائة ساكن دون التراجع في الأرقام، فكلما تقدمت السنوات كلما ارتفع عدد مستخدمي الانترنت سواء في الدول المتقدمة أو الدول النامية، مما يستلزم النمو المستمر في أعداد مستخدمي الانترنت على المستوى العالمي أيضا، ولذلك يمكننا تصور التعداد الهائل الذي يشكله المجتمع المعلوماتي على المستوى العالمي والذي لا يزال في التزايد كلما تقدم الزمن، وبالمقابل فإنه يمكننا أيضا تخيل حجم الأضرار التي يتعرض لها المجتمع المعلوماتي جراء الجرائم الالكترونية التي تستهدفه.

الفرع الثاني: المؤشرات الإحصائية عن الجرائم الإلكترونية

لقد أجريت دراسة عام 2011 م حيث بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة تأثَّر بها 589 مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 9% من إجمالي سكان العالم. وقد توزَّعت هذه الجرائم

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

ما بين جرائم الفيروسات والبريد الإلكتروني الضار، وجرائم الاحتيال والنصب والاصطياد الالكتروني، والجرائم المتعلقة باختراق الهواتف المحمولة.[1]

كما كشف تقرير مشترك نشرته شركة "مكافي" McAfee الأمنية بالتعاون مع مركز الدراسات الاستراتيجية والدولية[2]، بأن حجم خسائر الاقتصاد العالمي الذي تسببه الجريمة الإلكترونية يتراوح سنويًا مابين 300 مليار إلى 1 تريليون* دولار أمريكي، ويكلف اقتصاد الولايات المتحدة لوحدها مابين 24 إلى 120 مليار دولار سنويًا، وهو ما يُقدّر بحوالي 0.2 إلى 0.8 من الناتج المحلي الإجمالي للولايات المتحدة الأمريكية.

وفي دراسة قامت بها نورتن Norton التابعة لشركة سيمانتيك Symantec المتخصصة في أمن المعلومات بالتعاون مع شركة "ستراتيجي ون" Strategy one بدارسة إحصائية لسلوك الفيروسات في 42 دولة من بينها دولة الإمارات العربية المتحدة وذلك في 18 سبتمبر 2011 [3]، حيث أظهر تقرير الدراسة أن شخصين، على أقل تقدير من القاطنين بدولة الإمارات العربية المتحدة يقعون ضحية أنشطة الجريمة الإلكترونية في الدقيقة الواحدة بفعل الفيروسات ورسائل التحايل الإلكترونية، وهجمات اصطياد المعلومات السرية والمصرفية وغيرها، أي أكثر من 1.4 مليون مستخدم في الإمارات يتعرضون لهجمات إلكترونية يوميا.

وقدّر التقرير أن خسائر قيمتها 209 مليون دولار سنويا ناتجة عن الهجمات الإلكترونية في الإمارات ومتطلبات إصلاح الأضرار المترتبة عليها، ويشير تقرير نورتن إلى أن أكثر أشكال الجريمة الإلكترونية انتشاراً بالإمارات هي الفيروسات أو البرمجيات الخبيثة التي تستهدف الحواسيب بنسبة 51%، تليها رسائل الاحتيال الإلكترونية بنسبة 19 %، ثم هجمات اصطياد المعلومات الخاصة والسرية بنسبة 18 %، حيث تعتمد أنشطة الجريمة الإلكترونية على رسائل الاحتيال الإلكترونية وهجمات

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

اصطياد المعلومات الخاصة والسرية لسرقة المعلومات المصرفية وبيانات البطاقات الائتمانية لاستغلالها في أغراض إجرامية.

كما أن نسبة الجرائم الإلكترونية التي يتعرض لها مستخدمو الإنترنت في الإمارات أكبر منها بكثير مقارنة بالجرائم التقليدية، إذ تبلغ نسبة من تعرّضوا لجرائم إلكترونية 55% مقارنة بـــ18% فقط من الذين تعرضوا لجرائم تقليدية.

ويشير التقرير إلى أن قرابة 20% من كافة أنشطة الجريمة الإلكترونية بالإمارات تستهدف الأجهزة النقالة خاصة وأنه قرابة 56% من مستخدمي الهواتف النقالة في الإمارات يستعملون هواتفهم النقالة للنفاذ إلى الإنترنت مما يؤكد الحاجة إلى أخذ الحيطة اللازمة مع ازدياد الهجمات التي تستهدف هذه الأجهزة وانتشارها بوتيرة متسارعة.

ولقد وصلت الخسائر المتراكمة من الجرائم الإلكترونية بالمملكة العربية السعودية[1] إلى 1.9 مليار ريال سعودي، وتقدر خسارة المستخدم السعودي الذي يقع ضحية لأعمال قرصنة أو تجاوزات غير شرعية عبر الشبكات الإلكترونية بـــ 697 ريالاً للضحية الواحدة جراء الجريمة الإلكترونية.

وقد نشرت جريدة "المستقبل العربي"[2] الالكترونية تقريرا صدر من شركة "سيمونتيك" صنفت فيه الجزائر في المرتبة 61 عالميا من بين الدول التي تتعرض للجريمة الإلكترونية.

وما نخلص إليه أن المؤشرات المتعلقة بالأضرار الناتجة عن الجرائم الالكترونية ما هي إلا بعض من الأمثلة التي تصور لنا ضخامة الخسائر المنجرّة عنها، فالجرائم الإلكترونية لا تطال الاقتصاد القومي أو التكنولوجيا فقط، بل تتعدى حدودها إلى المساس بالمجتمعات والأشخاص، والممتلكات والأعراض، والأموال، والأفكار، والإيديولوجيات وكل ما له صلة بالحياة المدنية، وهي تختلف باختلاف الدوافع الإجرامية، كما تتسم بالتكاثر والتطور المستمر في ابتكار طرق الاحتيال كلما تقدمت التكنولوجيا.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الباب الثاني

أنواع الجرائم الإلكترونية وآثارها

الفصل الأول: الجرائم الإلكترونية المتعلقة بأمن المعلومات

الفصل الثاني: الجرائم الإلكترونية المتعلقة بالأموال والأشخاص

الفصل الثالث: الجرائم الإلكترونية المتعلقة بأمن الدول
و المجتمعات

1)
2)
..

تمهيد:

إن سرعة تكيف الجرائم الإلكترونية مع تكنولوجيا المعلومات شكل عائقا كبيرا في الاستقرار على معيار واحد في تصنيفها كأن تصنف على أساس ارتكاب الجريمة، أو تصنف على أساس دوافع المجرم، أو على أساس محل الجريمة، أو تصنف على أساس المعيار الوظيفي الذي يقوم على دور الكمبيوتر ونظمه كوسيلة مباشرة وغير مباشرة للجريمة.

ونظرا لخطورة الظاهرة برزت عدة مسارات عالمية جديدة تسعى إلى وضع تصنيفات معينة للجرائم الإلكترونية بهدف تحقيق التعاون الدولي لمكافحتها وقد جمع لهذا الغرض أكثر من معيار تصنيفي لتقسيم هذه الجرائم؛ كاعتبار دور الكمبيوتر ونظمه معيارا لها، أو اعتبار الجرائم المرتكبة وغايتها، أو اعتبار ارتباطها بالأشخاص والأموال..، و في هذا الشأن تمخض عن مشروع الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت تصنيف الجرائم المعلوماتية وفق أقسام أربعة:[1]

1 ــ جرائم ترتبط بالكمبيوتر كالتزوير والاحتيال المعلوماتي.

2 ــ جرائم تستهدف نظم الكمبيوتر ومكوناته كالدخول غير المصرح به واعتراض أنظمته أو تدمير مكوناته، وإساءة استخدام الأجهزة المعلوماتية.

3 ــ جرائم مرتبطة بالإخلال بحق المؤلف والحقوق المجاورة وقرصنة البرامج.

4 ــ جرائم مرتبطة بالأفعال الغير أخلاقية والإباحية.

كما تصنف الجرائم الإلكترونية باعتبار تعلقها بأمن المعلومات، وتعلقها بالأموال والأشخاص، وتعلقها بأمن المجتمعات، وهو التنصيف الذي اخترته في دراستي لما يخدم البحث.

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الأول:
الجرائم الإلكترونية المتعلقة بأمن المعلومات

المبحث الأول: الجرائم المستهدفة للحواسيب

المبحث الثاني: جرائم تطوير الفيروسات ونشرها

المبحث الثالث: جرائم تدمير المواقع الإلكترونية

المبحث الرابع: جرائم اختراق البريد الإلكتروني وقرصنة البرامج

المبحث الخامس: جريمة التزوير الإلكتروني

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: الجرائم المستهدفة للحواسيب

أجري تقرير عام 1994م جاء فيه أن الحواسيب في الولايات المتحدة تحتفظ بأكثر من خمسة مليارات من التسجيلات المتضمنة لمعلومات تخص كل رجل وامرأة وطفل، وكمثال واحد فقط فإن سجل البيانات الائتمانية يحتوى على أكثر من 400 مليون ملف ائتماني، يتم تحديثها بأكثر من ملياري قيد في كل شهر وهو ما يعجز الإنسان عن تحقيقه يدويا[1]، وبالرغم من أهمية الحواسيب فإنها تتعرض لجرائم متعددة تستهدف محتوياتها ومكوناتها وفق دوافع مختلفة، والمطالب التالية تبين أبرز هذه الجرائم شيوعا:

المطلب الأول: جريمة الدخول غير المصرح به إلى الحاسوب.

يشمل مصطلح الدخول غير المصرح به إلى الحاسوب كافة الأفعال التي تسمح بالدخول إلى نظام معلومات الحاسوب والإحاطة به أو السيطرة على معطياته التي يتكون منها، أو الاستفادة من الخدمات التي يقدمها، فعدم مشروعية الدخول إلى أنظمة الحاسوب تعود إلى عدم الترخيص بذلك Unauthorized Access [2]، حيث يجرم القانون الوصول إلى البيانات والمعلومات* المخزنة داخل الحاسوب بدون علم أو رضا المسئول عنها[3]، وقد جاء في اتفاقية بودابست المتعلقة بمكافحة جرائم المعلوماتية عام 2001م في المادة الخامسة منها على أنه " يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبار الدخول المتعمد لكل أو لجزء من نظام الحاسب الآلي بشكل غير مشروع، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن بنية الحصول على بيانات الحاسب الآلي أو أي نية إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آخر"[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

فعلة تجريم الدخول غير المصرح به إلى أنظمة الحاسوب المعروفة بالاختراق[1]، مردها التهديد الذي يستهدف أمن النظام المعلوماتي وسريته وسلامته، كالوصول إلى البيانات السرية أو كلمات المرور Access Codes أو معلومات خاصة بالنظام المستهدف والتي تسمح بتدميره أو إتلاف بياناته بغض النظر عن الاختراق إن كان عن طريق شبكة محلية أو شبكة الانترنت.

ولذلك تشترط مذكرة بودابست بأن الدخول المصرح به يجب أن يتم بإذن من مالك النظام أو كل من يخول له الحق فيه، مع العلم أنه لا يجرم الدخول إلى الأنظمة المتاحة للجمهور باعتبار الدخول إليها حقا من الحقوق وهو تصريح ضمني[2].

المطلب الثاني: أركان جريمة الدخول غير المشروع للحواسيب.

الفرع الأول ــ الركن المادي:

يتحقق الركن المادي وفق صورتين؛ الأولى هي الدخول المباشر Direct Acces باستخدام الحاسوب المستهدف للحصول على المعلومات التي يحتوي عليها، والصورة الثانية هي اختراق الحاسوب للحصول على المعلومات عن طريق نظام آخر يتصل بالحاسوب عن طريق شبكة الإنترنت[3].

وكي يقوم الركن المادي للجريمة يجب أن يتحقق الاتصال الفعلي من الجاني بالهدف، بمعنى أن الركن المادي لا يتحقق إذا قام الجاني بإجراء احتمالات لاكتشاف مفتاح الدخول المعروف بكلمة المرور، لكن بمجرد اختراقه للحاسوب يصبح الركن المادي قائما حتى ولو لم يستطع الوصول إلى البرامج أو المعلومات المستهدفة، بل يكفي مجرد دخوله غير المشروع إلى الحاسوب اعتبار ذلك جريمة في حد ذاتها لكونها تعديا محتملا على الحق، وهو ما تدعمه أغلبية التشريعات الوضعية التي تنص بأن فعل الدخول يكون قد انطوى على المساس بحق المسئول عن النظام في السيطرة عليه، بغض النظر عن

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المساس بسرية المعلومات التي يتضمنها النظام[1]، بينما التشريع الأمريكي يشترط كي تقوم الجريمة لابد أن يتم الوصول إلى المعلومات التي يتضمنها النظام المعلوماتي[2].

أما في حالة الدخول غير المصرح به عن طريق الخطأ، كأن يطلب المستعمل خدمة ما فيجد نفسه داخل نظام حاسوب غير مصرح له بالدخول إليه فإنه يتعين عليه الخروج الفوري من النظام، أما إذا تبين له ذلك وأصرّ على عدم الخروج فالنتيجة الإجرامية تكون واحدة لأن علة التجريم هي حماية النظام المعلوماتي[3].

الفرع الثاني ــ الركن المعنوي:

يمثل الركن المعنوي صورة القصد الجنائي المتعمد، ولا يتحقق القصد الجنائي إلا إذا توفر عنصري العلم والإرادة، أي علم الجاني بعدم مشروعية الدخول إلى النظام المستهدف لاعتباره حق يحميه المشرع فإذا انتفى هذا العلم انتفى معه القصد الجنائي[4]، وأيضا يتطلب القصد الجنائي توقع الجاني النتيجة الإجرامية المترتبة على تصرفه وهي الدخول غير المشروع إلى النظام المعلوماتي بغض النظر عن الضرر الذي سيلحقه، ففرضا لو ادعى الجاني بأن دخوله غير المصرح به كان بباعث الكشف عن أوجه القصور في النظام الذي اخترقه من أجل إصلاحه مستقبلا، فإن فعله يجرم نظرا لتحقق النتيجة الإجرامية وهي الدخول غير المشروع إلى النظام المعلوماتي[5].

المطلب الثالث: صور الدخول غير المشروع للحاسوب وآثارها.

إن الحاسوب لا يميز بين دوافع الخير والشر، ولذلك يستجيب لأي جهة كانت بمجرد فك مفتاح الدخول أو الاتصال به بأي وسيلة متاحة، الأمر الذي سهل استخدامه في الأغراض غير

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المشروعة كالتلاعب بالبرامج والبيانات، ومن صور الجرائم الواقعة على الحاسوب نتيجة الدخول غير المصرح به ما يلي:

الفرع الأول ــ سرقة البرامج المعلوماتية:

تستثمر الشركات المختصة في إنتاج البرامج المعلوماتية وتطويرها أموالا طائلة وعقولا فائقة الذكاء ناهيك عن استهلاك الوقت، وكنتيجة لاعتبارات معينة ــ كغلاء أثمانها ــ يتم اختراق الحواسيب لغرض سرقة هذه البرامج ونسخها بدون إذن ملاّكها وبيعها بأرخص الأثمان وهو ما أثر سلبا على الاستثمار في هذا المجال وأدى إلى إفلاس العديد من الشركات المتخصصة في إنتاج البرامج، حيث تشير الإحصاءات المتعلقة بالاختراقات أن هذه الظاهرة الإجرامية انتشرت في جميع أنحاء العالم بما فيها البلدان العربية والأفريقية، والجدول التالي يبين دول الشرق الأوسط والدول الإفريقية المتصدرة في سرقة البرامج المعلوماتية بالنسب المئوية، وذلك ابتداء من سنة 2004 إلى غاية 2008.[1]

جدول رقم(02): يبين حجم سرقة البرامج بالنسب المئوية في دول الشرق الأوسط والدول الإفريقية من سنة 2004 إلى غاية 2008 [2]

دول الشرق الأوسط والأفريقية	2004	2005	2006	2007	2008
الجزائر	% 83	% 83	% 84	% 84	% 84
البحرين	% 62	% 60	% 60	% 57	% 55
بوتسوانا ــ جنوب افريقيا ــ	% 84	% 82	% 81	% 82	% 80
الكاميرون	% 84	% 84	% 84	% 84	% 83
مصر	% 65	% 64	% 63	% 60	% 59
العراق	--	--	--	% 85	% 85
ساحل العاج	% 84	% 82	% 82	% 81	% 80
الأردن	% 64	% 63	% 61	% 60	% 58
كينيا	% 83	% 81	% 80	% 81	% 80
الكويت	% 68	% 68	% 64	% 62	% 61
لبنان	% 75	% 73	% 73	% 73	% 74
ليبيا	--	--	--	% 88	% 87
موريطانيا	% 60	% 60	% 59	% 57	% 57

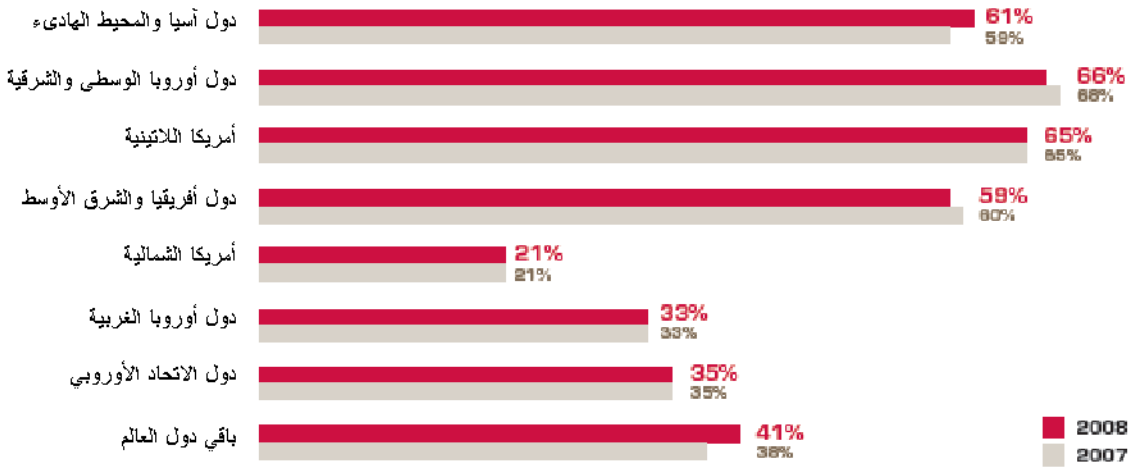
(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

المغرب	% 72	% 68	% 68	% 67	% 66
نيجيريا	% 84	% 82	% 82	% 82	% 83
عُمان	% 64	% 63	% 62	% 61	% 62
قطر	% 62	% 60	% 58	% 54	% 51
العربية السعودية	% 52	% 52	% 52	% 51	% 52
السنغال	% 84	% 82	% 81	% 80	% 79
جنوب أفريقيا	% 37	% 36	% 35	% 34	% 35
تونس	% 84	% 81	% 79	% 76	% 73
تركيا	% 66	% 65	% 64	% 65	% 64
الإمارات العربية المتحدة	% 34	% 34	% 35	% 35	% 36
اليمن	--	--	--	% 89	% 89
زامبيا	% 84	% 83	% 82	% 82	% 82
زمبابوي	% 90	% 90	% 91	% 91	% 92
بلدان أفريقية أخرى	% 84	% 84	% 85	% 85	% 86
بلدان أخرى في الشرق الأوسط	% 93	% 91	% 89	% 87	% 87

كما يترجم الشكل التالي حجم سرقة البرامج بالنسب المئوية وذلك حسب مناطق العالم خلال سنتي: 2007 و 2008.



شكل رقم(10): يبين النسب المئوية لسرقة البرامج حسب مناطق العالم خلال سنتي: 2007 و 2008.[1]

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

الفرع الثاني ــ اختلاس وإتلاف المعلومات:

يمثل اختلاس المعلومات الاستيلاء غير المشروع على المعلومات والبيانات من الحواسيب لأغراض متعددة تصب في مصلحة المخترقين أو من يستخدمهم، ومن صور إتلاف المعلومات Information Sabotage ؛ محو تعليمات البرامج أو البيانات، أو إدخال بيانات إضافية بغرض التشويش على صحة البيانات القائمة مما يؤدي إلى زوال المعلومات أو فقدان منفعتها لاختلال كفاءتها وصلاحيتها للاستعمال فيؤثر سلبا على قيمتها[1]، أما بواعث إتلاف المعلومات فهي عديدة ومن بينها الرغبة في الانتقام من شخص طبيعي أو معنوي عن طريق إعاقة نظم المعلومات عن أداء وظائفها مما يؤدي إلى خسائر كبيرة تضر بالضحايا، وكمثال حي على ذلك ما حصل في إيطاليا وفرنسا لما تم إتلاف عدد كبير من الحواسيب في مراكز للحسابات، وقد قدرت الخسائر في إيطاليا ما يعادل عشرة ملايين دولار أمريكي، وهو إجمالي الخسائر الناتجة عن الاعتداءات على عشر مراكز متفرقة منذ عام 1976 إلى غاية 1978م، وفي فرنسا قامت جماعة إجرامية أطلقت على نفسها اسم (كلودو) (Clodo) بإتلاف عدد كبير من أجهزة الحواسيب في عدد من المؤسسات عامي 1980 و 1981م، وقدرت الخسائر المترتبة عن كل هجوم نحو مليون ونصف مليون فرنك فرنسي.[2]

الفرع الثالث ــ تعطيل خدمات الحاسوب:

من أهداف الدخول غير المشروع للنظام المعلوماتي إتلاف الأنظمة، مما يؤدي إلى إعاقة تدفق المعلومات والبيانات Dataflow فيتعطل جزء هام من أنظمة الحاسوب الأمر الذي يجعله يتوقف في العديد من الحالات عن تقديم خدماته بصفة نهائية أو لفترة من الزمن، وهذه الجريمة حتما ستعيق المستخدمين الشرعيين من الوصول إلى معلوماتهم أو الاستفادة من الخدمات بعد رفض الحاسوب تقديم الخدمة المطلوبة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني: جرائم تطوير الفيروسات ونشرها

يعود تاريخ ظهور الفيروسات ـــ البرامج الخبيثة ـــ إلى نهاية الأربعينات أين بقيت أضرارها محدودة بسبب عدم ربط الحواسيب بالشبكات[1]، أما المرحلة الخطيرة فكانت ابتداء من عام 1987م لما نشرت مجلة "نيوز داي" مقالا متخصصا في جرائم الحاسوب يتحدث عن ظهور ثلاثة فيروسات خلال شهرين متتاليين وهو ما أدى إلى الإسراع في إنتاج بعض برامج الحماية، وقد استفز هذا الأمر صانعي الفيروسات وجعلهم يقومون بابتكار برامج خبيثة أكثر ضراوة وأوسع انتشارا، وعلى إثرها بدأت حرب الفيروسات والبرامج المضادة.[2] وما زاد من حدة المشكلة أن الأدوات والمعارف اللازمة لتصميم برامج الفيروسات الخطيرة أصبحت اليوم معروضة على شبكة الانترنت، وتم طبع العديد منها على الكتب لتمد المهتمين بكل ما يحتاجون إليه من معلومات تتعلق بإنتاج الفيروسات الأكثر ضراوة.

المطلب الأول: مفهوم الفيروس

الفرع الأول: تعريف الفيروس في لغة المعلومات

يعد الفيروس من أهم الموضوعات التي شغلت بال المختصين والباحثين في مجال المعلوماتية، ولقد خلصت الدراسات إلى مجموعة من التعريفات المختلفة لفيروس الحاسوب وما يلاحظ عنها أنها تشترك في المفهوم التخريبي الذي يلحقه الفيروس بنظام الأمن المعلوماتي، ومن أهم هذه التعريفات ما يلي:

"الفيروس عبارة عن برنامج له أهداف تدميرية يهدف إلى إحداث أضرار جسيمة بنظام الحاسب سواء البرامج أو مكوناته"[3]، ونستخلص من التعريف أن الفيروس هو برنامج يتم تصميمه بإحدى لغات البرمجة المختلفة، ويحتوي على مجموعة من الأوامر التخريبية متفاوتة الخطورة كإلحاق الضرر بنظام المعلومات أو تدمير البيانات أو توقيف الحواسيب عن أداء مهامها أو إدخال تعديلات تخريبية على البيانات.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما يعرّف الفيروس بأنه: عبارة عن معلومة خاطئة أو أمر مضلل يدخله الجاني عن طريق وسائط التخزين أو الشبكة إلى الحاسوب لتعطيله عن منفعته التي أعد من أجلها. ويعرّف أيضا بأنه برنامج يتم زرعه على الأقراص والأسطوانات الخاصة بالحاسب، ويظل خاملا لفترة محددة ثم ينشط فجأة في توقيت محدد ليدمر البرامج والبيانات المسجلة و يمتد أثره التخريبي ليشمل الإتلاف والحذف والتعديل[1].

وعرّفه المركز الوطني للحاسب الآلي في الولايات المتحدة في تقرير أعده حول الاعتبارات الأمنية في الحواسيب بأنه: "برنامج يهاجم أنظمة الحاسب الآلي بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان وهو في العادة برنامج صغير مكتوب بلغة متدنية المستوى مثل "لغة التجميع" مما يزيد من صعوبة اكتشافه، ويقوم الفيروس بالتجول في الحاسب الآلي باحثا عن برنامج غير مصاب، وعندما يجد واحدا ينتج نسخة من نفسه لتدخل فيه، وتتم عملية الإدخال هذه في جزء من الثانية، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ أوامر الفيروس"[2].

الفرع الثاني ــ أصناف الفيروسات:

لقد أصبح من الصعب حصر فيروسات الحاسوب لأنها تعد بمئات الآلاف كما يسجل في كل يوم ظهور أنواع جديدة منها، وهو ما جعل المختصين يصنفونها بحسب أهدافها كما يلي:

1 ــ فيروس عام العدوى: وهو ينتقل إلى جميع البرامج أو الملفات ويهدف إلى تعطيل نظام التشغيل بكامله.

2 ــ فيروس محدد العدوى: وهو يستهدف نوعا معينا من النظم لمهاجمته، ويتميز بالبطء في الانتشار علاوة على صعوبة اكتشافه.

3 ــ فيروس عام الهدف، ويتميز بسهولة إعداده واتساع مدى تدميره وتندرج تحته غالبية الفيروسات المعروفة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

4 ــ فيروس محدد الهدف: وهو نوع من الفيروسات التي تقوم بتغيير مجال عمل البرامج دون تعطيلها، ويحتاج إنتاج هذا النوع من الفيروسات إلى مهارة عالية في مجال المعلوماتية.[1]

الفرع الثالث: خصائص الفيروسات

من أجل تحقيق أهداف البرامج الخبيثة ــ الفيروسات ــ فإنها تبرمج وفق خصائص هجومية ودفاعية في آن واحد، حيث تخترق الهدف خفية ثم تبدأ بتفعيل نشاطها التخريبي، ومن أهم خصائصها:

1 ــ آلية التناسخ The Replication Mechanism ، فيكفي نشر الفيروس على حاسوب واحد وعند تفعيله يبدأ بخاصية التناسخ التلقائي في جميع الحواسيب التي تتصل بالضحية عن طريق الشبكات أو أي وسائط اتصال أخرى.

2 ــ آلية التخفي The Protection Mechanism ، فالكثير من الفيروسات يتم نشرها في الحواسيب عن طريق إخفائها في أحد البرامج المطلوبة لدى المستخدمين، حيث تنشط مباشرة بعد تثبيت البرنامج المطلوب أو تفعيله، وفي حالات أخرى يتم دسها خفية في أنظمة الحواسيب أو الوسائط ذات الصلة بها وكي لا يكتشف أمرها لا تُفعل إلا بعد مدة محددة.

3 ــ آلية التنشيط The Trigger Mechanism ، وهي من الخصائص البارزة للفيروسات خاصة المدمرة منها والتي يطول ضررها أكبر حد ممكن من الأنظمة المعلوماتية، حيث تبرمج بتفعيل نشاطها آليا وفق توقيت أو تاريخ معين لتفاجئ الضحايا في وقت واحد.

4 ــ آلية التنفيذ The Payload Mechanism ، وهي خاصة أيضا تتميز بها الفيروسات في تنفيذ مهامها التخريبية للأهداف الموجهة إليها.

ورغم كون الفيروسات لا تُفعل من خلال البيانات، إلا أنها تتشكل في صورة برامج مصغرة "ماكروMacro" يتم إلحاقها ببيانات الملفات "كالوثائق مثلا" files، وعندما يقوم المستخدم بتشغيل برنامج معالجة النصوص على سبيل المثال كبرنامج الوورد word لقراءة الملف المعني، يتم التشغيل الآلي لذلك "الماكرو" Macro المدمج ضمن الملف وبذلك يتمكن الفيروس من العمل، ومن أمثلة الفيروسات

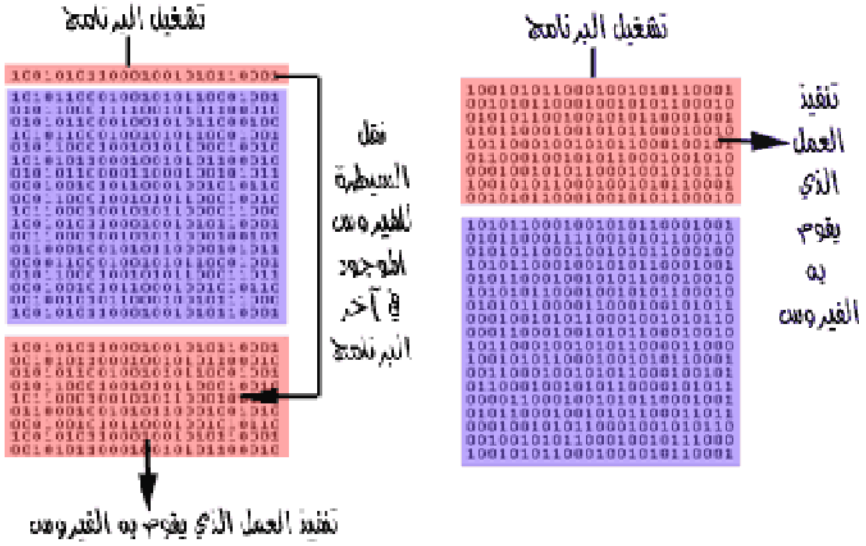
---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

التي تنتهج هذه الطريقة فيروس Impostor، وفيروس Wazzy، وفيروس الكلب المجنون Maddog هذا الأخير الذي يقوم بتغيير حرف a إلى e في كامل الوثيقة مهما كان عدد صفحاتها، وقد برمج هذا الفيروس بأن يبدأ عمله التخريبي كل يوم في الساعة الثامنة مساء.



شكل رقم(11): يمثل عملية تفعيل الفيروس الملحق بالملف مباشرة أثناء تشغيل البرنامج

المطلب الثاني: أنواع فيروسات الحواسيب

هناك مئات الآلاف من أنواع فيروسات الحواسيب؛ فمنها ما يبدأ عمله التخريبي مرتبطا بوقت أو حادثة معينة، ومنها ما يتكون من أجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري، ومنها ما يكون متخفيا حتى عن برامج مكافحة الفيروسات[1]، والفروع التالية تبين أشهرها وأكثرها انتشارا:

الفرع الأول ــ الديدان Worms :

فيروس الدودة هو من البرامج الخبيثة malwares التي تستغل أية فجوة في نظم تشغيل الحواسيب لتبدأ بنشاطها، كما تنتقل من حاسوب إلى آخر ومن شبكة إلى أخرى عبر الوصلات التي تربط بينها، وتتكاثر أثناء انتقالها كالبكتيريا وذلك عن طريق الانتشار والاستنساخ التلقائي لها، ويهدف هذا النوع من البرامج إلى إضعاف كفاءة الشبكة المعلوماتية أو التخريب الفعلي للملفات والبرامج ونظم التشغيل، وتختلف في طريقة عملها من نوع لآخر حيث يتناسخ بعضها داخل الحاسوب إلى أعداد هائلة بينما ينتشر بعضها الآخر عبر البريد الإلكتروني، وتكمن خطورتها في عدم

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../.....

اعتمادها على أي برنامج ملحق مما يعطيها الحرية الكاملة في الانتشار السريع وإلحاق أضرار كبيرة بالأجهزة والشبكات. فبإمكانها أن تنتقل عبر برامج المحادثة الفورية كبرنامج السكايب skype، كما تستغل قائمة عنوانين البريد الالكترونية للضحية لترسل نفسها إلى جميع العناوين المخزنة لدى جهاز الضحية وبذلك تصيب أكبر عدد ممكن من الأجهزة عبر البريد الإلكتروني ثم تكرر نفس الطريقة لدى كل مرسل إليه، ومن أثارها إبطاء خدمة شبكة الانترنت أو انقطاعها كليا، كما تسمح بفتح روابط خاصة بالأجهزة المخترقة لسحب المعلومات منها... [1]

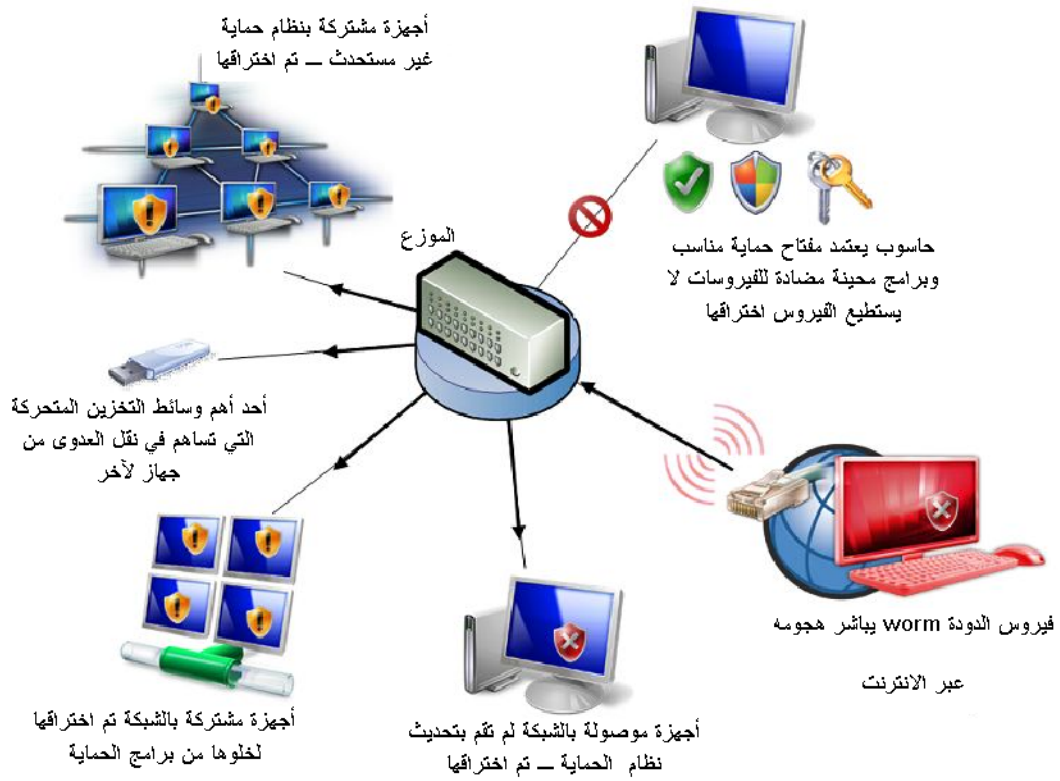
ومن أخطر أنواعها دودة كونفيكر Conficker worm التي انتشرت في ما يقرب من 9 ملايين كمبيوتر في أقل من 4 أيام! ويعود سببها إلى تحديث أجرته شركة ميكروسوفت Microsoft لأنظمة التشغيل الخاصة بها مثل: Windows XP و VISTA بهدف معالجة ثغرة أمنية في أنظمة التشغيل، وقد أتاحت ميكروسوفت لعملائها تحميل هذا التحديث لحماية أجهزتهم من الاختراقات، وكما هي العادة لم يول الكثير اهتماما بالتحميل أو تحديث الأنظمة! وهو ما استغله مبرمجو هذه الدودة الذين استفادوا من اكتشاف الثغرة الموجودة في الأنظمة وأسرعوا في نشرها عن طريق شبكة الإنترنت حيث تم اختراق الأنظمة التي لم تعتمد تحديث ميكروسوفت، وبدورهم ساهموا في الانتشار التلقائي للدودة في جميع الأجهزة الموصولة، ومن الآثار السلبية أيضا لهذه الدودة أنها تمكن المجرمين من اختراق أجهزة المستخدمين وتنفيذ أعمالهم الإجرامية قبل أن يتفطن الضحايا! والشكل التالي يوضح طريقة انتشار فيروس الدودة بالنسبة للأجهزة التي لم تفعل وسائل الحماية الأمنية. [2]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...



شكل رقم(12): يبين طريقة انتشار فيروس الدودة بالنسبة للأجهزة التي لم تفعل وسائل الحماية الأمنية أو لم تحيّنها[1]

وقد جاء في مثال حي أن طالبا جامعي يدعى روبرت موريس Robert Morris متخصص في علوم الكومبيوتر بجامعة كورنيل الأمريكية Cornell Unversity بولاية نيويورك، قام بنشر برنامج دودة الانترنت Internet Worm كي يثبت عدم ملائمة وسائل الحماية في شبكات الحاسوب، غير أنه تسبب في تدمير وإتلاف الآلاف من شبكات الحاسوب المنتشرة في الولايات المتحدة إضافة إلى إعاقة مسالك هذه الشبكات، وقد كلّف إعادة البرمجة ملايين الدولارات[2]. وتمت محاكمة موريس بموجب القانون الذي يجرم الدخول إلى المواقع الحكومية بدون تصريح، حيث أدين بوضعه تحت الرقابة القانونية لمدة ثلاث سنوات مع القيام بخدمة المجتمع لمدة 400 ساعة مع تغريمه مبلغا قدره عشرة آلاف وخمسين دولارا أمريكيا.[3]

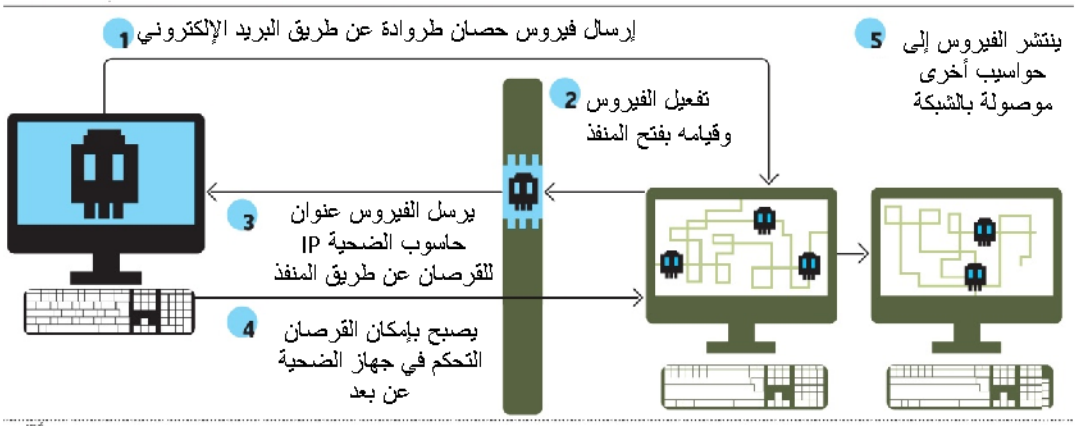
(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني: فيروس حصان طروادة Trojan Horse

هو برنامج خبيث يتستر ببرنامج آخر سليما أو رسالة إلكترونية، ولما يقـــوم المستخـــدم بتثبيت البرنامج السليم في الحاسوب وتفعيله أو فتح الرسالة الإلكترونية، ينفصل برنامج حصان طروادة ليبدأ نشاطه آليا، وفي الغالب يكون الهدف من فيروس حصان طروادة هو فتح أحد منافذ الحواسيب كمنفذ خلفي backdoor يتيح الفرصة للقراصنة وغيرهم من اختراقها والسيطرة عليها، ومن آثاره تمكين القراصنة من سرقة كلمات المرور password ، وسرقة المعلومات الحساسة المخزنة بالجهاز، كما يمنح الصلاحيات الكاملة للقراصنة من التجسس على الجهاز ومحتوياته والتجسس على جميع تصرفات المستخدم أثناء استخدامه المباشر للحاسوب، كما يعمل على تعطيل أجهزة استقبال وتوزيع خدمة الانترنت والشبكات، إضافة إلى ما يحدثه من اضطراب في عمل أجهزة الحاسوب كالتشغيل العشوائي لسواقات الأقراص المضغوطة والفأرة وغيرها..[1]



شكل رقم(13): يبين طريقة انتشار فيروس حصان طروادة ونشاطه

الفرع الثالث ــ القنابل المنطقية Logic Bombs :

هي برامج خبيثة يتم إدراجها خفية مع برامج سليمة بهدف تدمير أنظمة تشغيل الحواسيب أو إحداث تغييرات في برامج ومعلومات النظام، والقنابل المنطقية تبقى ساكنة ويتم تفعيلها التلقائي بمجرد حلول الوقت أو التاريخ المبرمج لها، كما قد يتم تفعيلها بتوافر شروط منطقية معينة داخل برنامج أو ملف معين وذلك وفقا للرمز الذي يحدده برنامج القنبلة، فبمجرد توفر الشرط المنطقي يبدأ

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../.....

برنامج القنبلة بمهامه التخريبية[1]، ومن الأمثلة الواقعية التي استخدمت فيها القنابل الزمنية ما قام به أحد المحاسبين المتخصصين في نظم معلومات الحاسوب؛ حيث وضع قنبلة زمنية في أنظمة شبكة المعلومات الخاصة بالشركة التي تم تسريحه منها وذلك بدافع الانتقام، وبعد ستة أشهر من تركه للشركة تم التشغيل التلقائي للقنبلة وأدى ذلك إلى إتلاف كل البيانات المخزنة في حواسيبها [2].

الفرع الرابع ــ فيروس باب المصيدة Trapdoor :

هو برنامج خبيث ينشر عمداً لتجاوز نظم الأمن والحماية في الحواسيب، حيث يزرع أثناء معاينة بعض البرامج أو تجريبها، كما يتم زرعه عند تنصيب البرامج الحساسة خاصة منها برامج الحماية ويبقى ساكنا حتى يقرر المخرب استخدامه، وبعد تفعيله يفتح ثغرة للدخول إلى أنظمة الحاسوب المحمية عن طريق تعطيله إجراء الفحوصات المعتادة، وهو أيضا يعد من الفيروسات البالغة الخطورة لكونه يتخطى برامج الحماية[3]، ومن الأمثلة العملية لهذا الفيروس أن أحد المبرمجين قام بإعداد برنامج الرواتب على نحو يسهل له إجراء اختبارات معينة على البيانات المدخلة للتأكد من صحة أوامر البرنامج وذلك بتغيير مسار البرنامج إذا تم إدخال حرف E ضمن الأرقام المدخلة من لوحة المفاتيح إلى حقل معين، وقد اكتشف أحد مستخدمي النظام هذه الثغرة فاستغلها بأن أضاف مبالغ كبيرة إلى راتبه من خلال إدخاله لأجور إضافية وهمية[4].

الفرع الخامس ــ فيروسات العتاد (Hardware Viruses)

يهدف هذا النوع من الفيروسات إلى تعطيل عتاد الحواسيب، حيث يبرمج الفيروس بأن يقوم بتنفيذ ملايين العمليات الحسابية اللامتناهية بطريقة تلقائية مما يلقي عبئا كبيرا على وحدة المعالجة المركزية* CPU وهو ما يؤدي إلى ارتفاع درجة حرارتها ثم تخريبها[5]، وبالتالي يتوقف الحاسوب نهائيا

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

عن العمل ولنتصور حجم الخسائر التي يحدثها هذا النوع من الفيروسات التخريبية لو يعطل حواسيب ملاحة الطائرات أو البواخر وغيرها..[1].

المبحث الثالث: جرائم تدمير المواقع الإلكترونية

يقصد بتدمير المواقع؛ الدخول غير المشروع من أي نقطة ارتباط أساسية أو فرعية متصلة بالانترنت من خلال نظام آلي Server – PC أو مجموعة نظم مترابطة شبكيا Intranet بهدف تخريب نقطة الاتصال أو النظام[2].

المطلب الأول : أشكال تدمير المواقع الإلكترونية

استطاع قراصنة الشبكات تخريب العديد من المواقع الإلكترونية خاصة الحيوية منها، وهو ما ألحق أضرارا جسيمة بالكثير من المصالح العامة على المستوى المحلي والعالمي كتعطيلهم لبوابات التجارة الإلكترونية التي نتج عنها خسائر بلغت ملايين الدولارات، ومن صور الجرائم التي تمس المواقع الإلكترونية ما يلي:

الفرع الأول ــ تدمير الموقع عن طريق استهلاك إمكانياته ومواده

يحصل ذلك عن طريق إرباك ذاكرة الخادم* الخاص بالموقع حيث تتعاون مجموعة كبيرة من شركاء الهاكرز بدخولهم الموقع في وقت واحد، ويستهدفون محرك البحث الموجود بالموقع سواء كان خاص بالموقع أو خاص بالشركة المستضيفة أو خاص بأي موقع آخر، ويقومون بإرباك باحث الموقع بكتابة كلمات متداولة الانتشار مثل: (what, how, when, with, on, in, where, why, who) وغيرها من الكلمات الاستفهامية، علما أن هذه الكلمات إذا أدخلت مرة واحدة وبشكل مستمر: فإن الخادم يعجز عن الاستجابة لكل الطلبات نظرا لكثافتها، فينهار الخادم وهو ما يؤدي إلى تعطل بنيته التحتية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وبالتالي تتوقف خدمة الموقع بصفة مؤقتة أو نهائية.

الفرع الثاني: إغراق موقع الضحية برسائل البريد

هي طريقة تشبه الأولى من حيث تكاتف مجموعة كبيرة من الهاكرز الذين يقومون بتسجيل أنفسهم داخل الموقع بأسماء وهمية للحصول على خدمة البريد المجاني الذي يتيحه الموقع المستهدف، وبالتنسيق بين الهاكرز في وقت واحد يقومون بإرسال مجموعة هائلة من الرسائل المرفقة بأحجام كبيرة من الملفات بصفة متكررة إلى نفس الموقع، فيسبب ذلك فيضان من الرسائل على الموقع وهو ما يعرف بـــ Flood ، وبطريقة أوتوماتيكية يحاول الخادم الاستجابة للخدمة المطلوبة للرد على الرسائل بشكل مستمر مما يفقده السيطرة بالنظر إلى الكم الهائل للرسائل فيتوقف عن الخدمة، وقد يستغرق استئنافه للعمل مدة طويلة وهو ما يفوت مصالح الناس.

الفرع الثالث ـــ استخدام الأوامر المركبة والمرجعية Ping

وهي من أكثر الطرق استعمالا لتدمير المواقع نظرا لقوة فعاليتها وسرعتها في نفس الوقت، كما أنها متاحة لدى جميع مستخدمي أنظمة windows و Linux حيث يستعين الهاكر بنافذة الدوس Dos لإرسال طلبات متكررة إلى الموقع الضحية عن طريق كتابة الأمر التالي: C :\windows>ping www.***-t والرمز (-t) هو أقصى معيار لكمية من الرسائل المرسلة، وبطريقة تلقائية يشرع الموقع الضحية بالرد لكنه يتوقف عن العمل نظرا لعدم تمكنه من الإجابة على الكم اللا متناهي من الرسائل، حيث تظهر رسالة لدى الهاكر تفيد تعذر الموقع عن الاستجابة نظرا للعطل الذي أصابه Requested time out مما يؤكد تعطل الموقع.

المطلب الثاني: أهداف تدمير المواقع الإلكترونية.

تختلف أهداف تدمير المواقع الإلكترونية حسب الدوافع التي يسعى من وراءها المهاجمين ومن أبرزها ما يلي:

1 ـــ قد يكون هدف تدمير الموقع بدافع التباهي والتفاخر لإثبات الذات والمقدرة الشخصية، وهو ما يحصل عادة على أيدي الهواة وطلاب الجامعات والمنبهرين بإمكانات التقنية الحديثة، ومثال ذلك ما قام به طالب أمريكي لم يتجاوز عمره الخمسة عشرة سنة من اختراق الحاسوب الرئيسي لمدرسته وقام بإحداث تعديلات في درجاته التي حصل عليها، وقد علّق على ذلك موقع CNN على

(1) الإحالات في النسخة المطبوعة.
(2) الإحالات في النسخة المطبوعة.

.../.....

الإنترنت: أن الطالب اقتحم الموقع ولكنه لم يغير درجاته إلى الأفضل لأن درجاته الأصلية كانت كاملة في جميع المواد وبالتالي قام بتغييرها إلى درجات قريبة من الرسوب، وقال الطالب: لم أستطع أن أفعل ما يقوم به المخترقون ولذلك فكرت أنه من المسلي أن أفعل عكس ما يفعلونه[1].

2 ــ التجسس السياسي والعسكري وحرب المواقع المضادة، فالكثير من الدول تسعى إلى الحصول على الأسرار العسكرية والأمنية لدول أخرى عن طريق التجسس الإلكتروني للإطلاع على الخطط العسكرية والإستراتيجية وإحباطها إذا ما اضطرت إلى ذلك ، خاصة وأن الحرب الإلكترونية لم تعد مجرد خيال علمي بل أصبحت واقعًا يهدّد الدول، وخير مثال على ذلك فيروس «ستاكسنت» الذي اخترق برنامج إيران النووي في أواخر شهر نوفمبر من عام 2010 وأدَّى إلى إيقاف الآلاف من أجهزة الطرد المركزي الخاصة بتخصيب اليورانيوم[2]، وهو فيروس يبحث في أجهزة الكمبيوتر التي يتسلل إليها عن طريق برنامج خاص طورته شركة سيمنز الألمانية فيتحكم بأنابيب النفط والمنصات النفطية في البحر ومحطات توليد الكهرباء وغيرها من المنشآت الصناعية[3].

3 ــ المنافسة بين الجهات المختلفة سواء كانت هذه المنافسة تقنية أو استخباراتية أو تجارية ولذلك يقول بعض خبراء الأمن المعلوماتي: إن الشركات التي تعتمد على الانترنت يجب أن تخشى من موظفيها السابقين والمنافسين أكثر من أي شيء آخر[4].

4 ــ سرقة بيانات مخزنة أو برامج، أو ملفات، أو التلاعب بموجودات أو أصول مالية كالحسابات البنكية وبطاقات الائتمان.

5 ــ دوافع أيديولوجية أو سياسية ضد منظمات أو جماعات أو دول، فعلى سبيل المثال: في أعقاب الهجمات على نيويورك وواشنطن في 11 سبتمبر 2001م، ارتفعت الأصوات في الولايات المتحدة والغرب تطالب بتدمير المواقع الإسلامية والعربية لاعتقادهم أنها تدعم الإرهاب أو تناهض الولايات المتحدة أو العالم الغربي عموما وقد شهدت المواقع العربية والإسلامية العديد من الاختراقات والتخريب[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الرابع: جرائم اختراق البريد الإلكتروني وقرصنة البرامج

لقد أصبح البريد الإلكتروني من وسائل الاتصال التي لا يستغنى عنها في الكثير من المجالات خاصة منها الاتصالات الثنائية كما قارب الهاتف من حيث الاستعمال، بل أصبح مستعملي الهاتف يستخدمون مراسلات البريد الإلكتروني أكثر من الاتصالات السمعية نتيجة انخفاض تكلفته في نقل المعلومات. هذه الأخيرة التي قد تكون في غاية الحساسية كتبادل خطط الشركات المستقبلية أو أسعار المنتجات التي سيتم عرضها أو استراتيجيات البيع، أو ربما المعلومات الفنية الخاصة بالتصنيع وغيرها من المعلومات الهامة، وبالمقابل فإن صناعة أمن المعلومات لم تغفل مجال الاهتمام بالبريد الإلكتروني والعمل على تأمينه، بل شجعت العملاء على تحصين معلوماتهم عن طريق تبني تقنيات أمن المعلومات وجعلتها في متناول الجميع كتقنيات التشفير المختلفة، وتقنيات المفاتيح التي تحتوي على الجدران النارية وغيرها، إلا أن الكثير من مستخدمي البريد الإلكتروني لا يأبهون بقضية الأمن، ويكتفون باستخدام كلمات المرور كوسيلة تأمين، وهي قطعا ليست مثالية[1].

المطلب الأول: صور اختراق البريد الإلكتروني.

على الرغم من أهمية خدمات البريد الإلكتروني فإن دراسة حديثة أكدت أنه مسئول عن نشر حوالي 80 بالمائة من الفيروسات في العالم باعتبار أن معظم الفيروسات مبرمجة لتستفيد من إمكانية الوصول إلى المستخدمين استعانة ببريد المستخدم[2].

ومن أشهر الانتهاكات التي تستهدف البريد الإلكتروني، إغراقه بالرسائل الوهمية حتى يعجز بريد الضحية من استقبال الرسائل الحقيقية الموجهة إليه، وذلك نتيجة إرسال آلاف الرسائل المرفقة بملفات ضخمة من حيث الحجم وتعرف هذه العملية بمصطلح E-Mail Flooding ، كما تتخذ هذه العملية شكل الهجوم المتعدد الأطراف وذلك عن طريق الإرسال المكثف للرسائل الإلكترونية من طرف العديد من الحواسيب المرتبطة بالانترنت ذات الوصلات السريعة، وهي عملية تؤدي إلى توقف

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

الحاسوب المستهدف نهائيا عن العمل نتيجة عجزه عن التعامل مع الكم الهائل للرسائل المتدفقة في آن واحد، ويطلق على هذا النوع من الهجمات بتفجير البريد الإلكتروني E-Mail Bombing [1].

هذا بالإضافة إلى انتهاك الخصوصيات الفردية التي يحتوي عليها البريد الإلكتروني بعد اختراقه، والغريب في الأمر أن بعض الجهات الأمنية الغربية تمتلك وسائلا جد متطورة تمكنها من اختراق أي بريد إلكتروني في العالم لمعرفة محتوياته والإطلاع على كل تفاصيل البريد الصادر والوارد المستهدف بحجة المراقبة الأمنية، ولكنها في نفس الوقت تعاقب كل من أطلع على الرسائل الإلكترونية، أو قام بسرقتها أو نشرها، أو تعمّد في إرسال فيروسات عبر البريد الإلكتروني للغير[2].

المطلب الثاني: أهداف اختراق البريد الإلكتروني.

لقد ثبت أن عمليات اختراق البريد الإلكتروني كثيرا ما تكون متعمدة بغرض تحقيق أهداف متفاوتة الخطورة والتي من بينها:

1 ـــ سرقة المعلومات ومفاتيح بطاقات الائتمان وأرقام الحسابات وغيرها، وقد تبين أن العديد من حالات القرصنة التي تطال الحواسيب يعود سببها إلى استغلال الثغرات التقنية التي يكتشفها القراصنة في برامج تشفير رسائل البريد الإلكتروني وهو دليل على سبق الإصرار [3].

2 ـــ التجسس سواء كان على الدول، أو المنظمات، أو الهيئات، أو المؤسسات أو الأفراد، وقد ورد في هذا الشأن تقرير نشر في جريدة الرياض الإلكترونية مفاده أن الإسرائيليين تجسسوا على الولايات المتحدة الأمريكية حيث استطاعت أجهزة الموساد اختراق الأنظمة الأمنية للبيت الأبيض واختراق شفرة البريد الإلكتروني الخاص بالرئيس الأمريكي، كما استطاعت أجهزة الموساد الوصول إلى شبكة الاتصالات في البيت الأبيض عبر اختراقها لمعلومات شركة كمبيوتر أمريكية كانت قد حصلت على حق تجديد شبكة معلومات لجهاز الطيران الحربي للإسرائيليين[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

3 ـــ المنافسة بين الدول أو الشركات أو المؤسسات أو الأفراد، ففي بعض الحالات يسعى مخترقي البريد الإلكتروني إلى الإطلاع على الرسائل الإلكترونية للمنافسين لهم الذين قد يمثلون هيئات قائمة بذاتها، وهدفهم في ذلك هو السعي نحو سرقة المعلومة التي قد تفيدهم في سبقهم إلى المشاريع وربح الصفقات.

4 ـــ سرقة الملفات أو الرسائل ذات الخصوصية الشخصية للتشهير بأصحابها بدافع الانتقام أو الفضول والعبث وقد يكون ذلك بدافع إثبات القدرة والتحدي على اختراق البريد الإلكتروني.

المطلب الثالث: جريمة قرصنة البرامج

تعتبر البرمجيات أحد المسببات الرئيسية التي جعلت من الحاسوب إحدى صور الحياة المعاصرة لما يقدمه من خدمات في جميع المجالات الاقتصادية منها، أو العلمية، أو الصحية وغيرها، وعلى هذا الأساس ثار جدل واسع بشأن طبيعتها وموضع حمايتها فنتج عن ذلك مدرستين؛ حيث تذهب الأولى إلى إصباغ البرامج سمة الاستغلال الصناعي باعتبارها منتج مادي وبالتالي فإن حمايتها لابد أن تكون في إطار قوانين براءات الاختراع، في حين تنظر المدرسة الثانية إلى البرامج باعتبارها أفكار وترتيبات لخوارزميات تتمثل في شكل ابتكاري وإبداعي، وبالتالي فإن حمايتها تكون ضمن حماية حقوق الملكية الفكرية، لكن هذا الاختلاف لم يكن إلا نظريا لأن أغلب التشريعات الدولية سارعت إلى حسم الجدل بإدراج برامج الحاسوب ضمن لائحة الأعمال الأدبية Literary Wok وأخضعتها لقوانين حق المؤلف، وبذلك شملتها الحماية القانونية كمصنف أدبي[1]، وهي حماية تحول دون تفاقم مشكلة القرصنة لبرامج الحاسوب.

وبالرغم من ذلك فإن البرامج لم تسلم بعد من جرائم القرصنة، حيث لا يكاد المستخدم يبحث عن برنامج إلا ويجد منه نسخا مجانية متاحة على الانترنت أو يتلقى عروضا بأثمان بخسة لا تقارن بالأسعار الفعلية للبرامج الأصلية، والأخطر من ذلك ما توفره الانترنت من مواقع إلكترونية متخصصة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

في نشر وتوزيع الوسائل المساعدة على كسر معظم أنواع الحماية للبرامج خاصة منها المعروضة للتجربة قبل البيع Trial Version ، ولقد اتخذت قرصنة البرامج صورا عديدة من بينها:

1 ــ استنساخ البرامج الأصلية بواسطة حارق الأقراص المضغوطة بدون إذن من مصدري البرامج الأصلية بغرض المتاجرة بها، وهي ظاهرة مستفحلة ومنتشرة عالميا، حتى أنه فتحت محلات علنية تبيع الآلاف من البرامج التي تم نسخها عن طريق الانترنت أو كسرت مفاتيح حمايتها بطرق غير مشروعة وتباع بأثمان جد بخسة مقارنة بأسعارها الحقيقية الأمر الذي شجع الطلب على هذا النوع من التجارة وكبد المصنعين خسائر كبيرة.

2 ــ استغلال البرامج الأصلية ذات الاستعمال الأحادي عن طريق تغيير بياناتها المثبتة من الجهة المصنعة لها، وهي حيلة تقنية تستعملها العديد من المنشآت التي تعتمد في تسيير نشاطها على برامج عالية الذكاء وباهظة الثمن حيث تعمد إلى شراء نسخة أصلية واحدة ثم تقوم بالتعديل غير المصرح به في بيانات البرنامج لتستفيد من خدماته في باقي ورشاتها، كما قد تتجرأ إلى بيع نسخ منه لمنشآت أخرى مما يعود بالضرر المادي على الجهات المصنعة للبرنامج.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الخامس: جريمة التزوير الإلكتروني

تتجسد جريمة التزوير الإلكتروني في أفعال الإدخال والمحو والتعديل، ولا يشترط اجتماعهما معا حتى يتوافر فيها النشاط الإجرامي لأن الركن المادي للجريمة يصبح قائما بمجرد القيام بفعل واحد، لكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو إحداث أي تعديل غير مصرح به[1].

المطلب الأول: مفهوم التزوير الإلكتروني

الفرع الأول ــ التعريف اللغوي للتزوير:

التزوير في اللغة تزيين الكذب، والتزوير إصلاح الشيء[2]، ومنه زور الكلام: زخرفه وموهه، وزور الكلام في نفسه: هيأه وحضره ومنه زور إمضاءه أو توقيعه: قلده[3] .

الفرع الثاني ــ تعريف التزوير في الاصطلاح الفقهي:

التزوير هو" تحسين الشيء ووصفه بخلاف صفته حتى يخيل إلى من سمعه أو رآه أنه بخلاف ماهو به، فهو ميل عن الحق وتمويه الباطل بما يوهم أنه حق"[4]. قال تعالى: ﴿فَقَدْ جَآءُو ظُلْمًا وَزُورًا﴾[5] أي افتروا على الله الباطل مع علمهم أنه باطل، وقالوا عن الحق أنه افتراء، فجعلوا الباطل حقا ونسبوه بعد ذلك إلى رسول الله ﷺ[6].

الفرع الثالث ــ تعريف التزوير في القانون الوضعي:

هو تغيير الحقيقة بقصد الغش، وبإحدى الطرق التي عينها القانون، تغييرا من شأنه أن يسبب ضررا للآخرين[7] ، كما يعرّف التزوير على انه تغيير الحقيقة في محرر بإحدى الطرق التي حددها

---

(1) الإحالات في النسخة المطبوعة.

(2) الاحالات في النسخة المطبوعة.

القانون تغييراً من شأنه إحداث ضرر بالغير وبنية استعمال هذا المحرر فيما زور من أجله[1].

كما يعرّف التزوير في القانون الجنائي بأنه تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر آخر بإحدى الطرق المادية أو المعنوية التي يبينها القانون، تغييراً من شانه إحداث ضرراً بالمصلحة العامة أو مصلحة شخص من الأشخاص[2].

فالعلة من تجريم التزوير هو حماية الثقة المنبعثة من المحررات بوصفها وسيلة التعبير عما تتضمنه من بيانات لتصبح في نظر الناس معبرة عن الحقيقة وبالتالي يقدمون على التعامل فيها بثقة واطمئنان مما يسمح للمحرر بأن يؤدي دوره بوصفه وسيلة السلطة العامة في مباشرة اختصاصاتها، ووسيلة الأفراد لإثبات علاقاتهم وكذلك إثبات حقوقهم المتنازع عليها[3].

الفرع الرابع ــ تعريف التزوير الإلكتروني وخصائصه:

أولا ــ تعريف التزوير الإلكتروني: يعرّف التزوير الإلكتروني بأنه أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في المخرجات الإلكترونية كالوثائق المحفوظة على وسائط التخزين، أو ورقية مطبوعة بعد معالجتها بالحاسوب، بشرط أن يكون المحرر الإلكتروني ذا أثر إثبات حق وأثر قانوني معين[4].

فتغيير الحقيقة هو الأساس الذي تقوم عليه جريمة التزوير، كوضع توقيع مزور على المستندات المعالجة آليا، أو الاستعانة بطرائق التزوير المعنوية كجعل واقعة مزورة في صورة واقعة حقيقية مثلا، كما ترتبط أيضا جريمة التزوير بأن تكون الوثيقة الإلكترونية ذات قيمة إثباتية وهذا يتفق مع القواعد العامة للجريمة التقليدية لإثبات الحقوق، إذ يشترط في المحرر المزور أن يكون أداة لإثبات حق من الحقوق[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ولذلك تعرّف الوثيقة الإلكترونية بأنها كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات وقد سجلت عليه معلومات معينة، سواء كان معدا للاستخدام بواسطة نظام المعالجة الآلية للمعلومات، أو كان مشتقا من هذا النوع[1]. وهو تعريف يوضح إمكانية حصول التزوير الإلكتروني سواء كانت مخرجات الحاسوب في صورة ورقية كالتي يتم إخراجها عن طريق الطابعة، أو بيانات رقمية مسجلة على الأقراص المضغوطة أو وسائط التخزين المعروفة، أو حتى المخرجات المبينة على وسائط العرض كشاشات الحواسيب[2].

ثانيا ـــ خصائص جريمة التزوير الإلكتروني:

يأتي في مقدمة خصائص جريمة التزوير الإلكتروني القصد الجنائي الخاص ـــ التزوير ـــ سواء في المحرر المعلوماتي أو سجلات الحاسوب عن طريق إدخال بيانات غير صحيحة بسجلات الحاسوب، أو سرقة منظومة التوقيع الإلكتروني واستخدامه بدلا من صاحبه الأصلي، وهو ما يشكل اعتداءا على النظام المعلوماتي؛ لأن القيام بذلك يتطلب الاختراق والتعدي والدخول على المواقع دون تصريح، أو استغلال التصريح في ارتكاب جريمة التزوير بإساءة استغلال الثقة، كما تعد جريمة التزوير الإلكتروني من الجرائم العابرة للحدود الجغرافية وتتطلب الاحترافية والمعرفة الفنية في اختراق الحواجز والوصول إلى المعلومات والبيانات قصد استعمالها في عمليات التزوير.

ومن أهم خصائص جريمة التزوير الإلكتروني عدم تركها لأي أثر مادي ظاهر يشير إلى مرتكبها، خاصة وأن سهولة إتلاف الأدلة الإلكترونية يجعل من الصعب تتبع مرتكبيها والقبض عليهم[3] .

المطلب الثاني: أساليب وصور جريمة التزوير الإلكتروني.

إن ما يتم تداوله في الحاسوب هو مجموعة من المعلومات ذات قيمة معينة قد تكون اقتصادية أو ثقافية أو مالية وغيرها، وهو ما يجعلها عرضة للسرقة أو محلا لجرائم التزوير أيضا، ولقد شهد التطبيق

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

العملي للحواسيب حالات كثيرة من التزوير كإبرام صفقات وهمية بأسماء أشخاص آخرين أو الحجز الوهمي لأماكن في شتى وسائل النقل، والفنادق، أو طلب شراء سلع أو خدمات بأسماء أشخاص وهميين، أو تحرير شهادات ووثائق مزورة في شتى الميادين، أو تزوير النقود الورقية باستعمال مدخلات ومخرجات الحاسوب، أو تزوير الماركات التجارية وبراءات الاختراع ، أو تزوير صور شخصية للتشهير بالغير أو لتضخيم الأحداث ونشر الفتن وغيرها..

وهناك وسائل متعددة تساهم في ارتكاب جريمة التزوير الإلكتروني، يأتي في مقدمتها استخدام ما يسمى بأدوات كسر كلمات المرور السرية كبرامج فك التشفير، كما تستخدم مولدات أرقام البطاقات الائتمانية للحصول على أرقام بطاقات الائتمان الخاصة بأي مودع ومن ثم القيام بعمليات الشراء باستخدام اسم ورصيد الضحية، كما تستغل الشبكات والعديد من البرامج المساعدة في سرقة المعلومات والبيانات ومن ثم استخدامها في جرائم التزوير الإلكتروني[1].

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

الفصل الثاني:
الجرائم الإلكترونية المتعلقة بالأموال والأشخاص

المبحث الأول: الجرائم الإلكترونية المتعلقة بالأموال

المبحث الثاني: الجرائم الإلكترونية المتعلقة بالأشخاص والآداب العامة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: الجرائم الإلكترونية المتعلقة بالأموال

تعد جرائم الاختلاس المرتكبة عن طريق الحواسيب من أبرز جرائم الاعتداء على الأموال التي تؤرق المشرعين ورجال القانون كونها لا تخضع لمعايير ومقاييس معينة كما يصعب التعرف عليها وفهم أبعادها وحيثياتها، ويشير مصطلح الاختلاس الإلكتروني إلى أي مخطط لجريمة سرقة المال يتم عن طريق استخدام التكنولوجيا الحديثة[1].

المطلب الأول: مفهوم جريمة الاختلاس الإلكتروني للأموال

الفرع الأول: تعريف الاختلاس في اللغة والاصطلاح

أولا: التعريف اللغوي للاختلاس:

الاختلاس لغة مشتق من الخلس وهو: الأخذ في نهزة ومخاتلة، يقال خلسه، يخلسه، خلسا، وخلسه إياه فهو خالس، ويقال " خلست الشيء واختلسته وتخلسته إذا استلبته".[2]

والاختلاس هو الاختطاف على وجه الاستلاب في حين غفلة من صاحب المال، تقول خلست الشيء خلسة: اختطفته بسرعة على غفلة.[3]

ولا يقتصر الاختلاس في اللغة على اختلاس المال بل يطلق على كل أخذ في نهزة وغفلة حتى أطلقه العرب على المتبارزين فقالوا عنهما إذا تبارزا: يتخالسان، لأن كل واحد منهما يختلس ضربة أو طعنة يقتل بها صاحبه، ويقال رجل مخالس أي شجاع حذر.[4]

ثانيا: تعريف الاختلاس في الاصطلاح الفقهي:

عرف المذهب الحنفي الاختلاس بأنه الأخذ من البيت سرعة وجهرا، وعرفوا المختلس بأنه: المختطف للشيء من البيت أو من يد المالك ويذهب.[5]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ويعرّف المالكية الاختلاس بأنه: أخذ المال والهرب به لا مغالبة.[1]

وعرّفوا المختلس بأنه: الذي يخطف المال بحضرة صاحبه في غفلته ويذهب بسرعة جهرا.[2]

كما عرّف الشافعية المختلس بأنه: الذي يأخذ الشيء عيانا ثم يهرب[3]، وقيل من يأخذ المال جهرة معاينة.[4]

ويعرّف الاختلاس عند الحنابلة بأنه: الخطف والنهب من غير غلبة[5]، والمختلس عندهم: الذي يخطف الشيء ويمر به.[6]

ثالثا: تعريف الاختلاس في القانون الوضعي

عرف فقهاء القانون الاختلاس بأنه: الاستيلاء على حيازة شيء بغير رضا مالكه أو حائزه[7] ، أو الاستيلاء على الحيازة الكاملة لمال الغير بغير رضا مالكه أو حائزه.[8]

وقيل هو الاستيلاء على الحيازة الكاملة للشيء بمفهومها المادي والمعنوي بدون رضا مالكه، وهو ما يتحقق من الناحية المادية بحرمان صاحب الحيازة القانونية منها[9]، بمعنى أن الاختلاس هو اعتداء على حيازة الغير.[10]

الفرع الثاني: مفهوم جريمة الاختلاس الإلكتروني للأموال

تعرّف جريمة الاختلاس الإلكتروني للأموال بأنها: "كل سلوك احتيالي ينتهج منهج الحوسبة، بنية الحصول على امتياز مالي"[11] وهو مصطلح استخدم في دراسة القانون باعتباره نموذج احتيالي Fraud scheme يستخدم فيه تطبيقات الانترنت التي تساعد على إحداث الاتصال بالغير، كالبريد الإلكتروني

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

e-mail ، والنشر التراسلي Message boards ، ومواقع التصفح Web sites وذلك قصد الإيقاع بالضحايا، سواء أكان الضحية شخصا طبيعيا أم معنويا.[1]

كما تستخدم أيضا حيلة الاصطياد الإلكتروني Phishing في اختلاس الأموال عن طريق إرسال كم هائل من الرسائل الإلكترونية الاحتيالية التي تطلب من المرسل إليه تحديث بياناته المصرفية وكأنها صادرة من البنوك والمؤسسات المالية، وبالتالي فإن كل ما يسجله الضحية من بيانات خاصة كالرقم السري ورقم الحساب وغيره يتم إرساله في حقيقة الأمر للمحتال وليس للبنك المعني.[2]

BNP PARIBAS

Cher client de **BNP Paribas**,

Le département technique de BNP Paribas procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.secure.bnpparibas.net/banque/portail/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© BNP Paribas 2006

شكل رقم: (14) يمثل رسالة إلكترونية صدرت سنة 2006م تدعو عملاء بنك BNP Paribas لتحيين ملفاتهم، وحقيقتها أنها رسالة احتيالية لاصطياد المعلومات الخاصة بالعملاء[3]

المطلب الثاني: صور جرائم الاختلاس الإلكتروني للأموال

الفرع الأول: اختلاس المبالغ الزهيدة

هي ظاهرة إجرامية مغرية، حيث يوهم المجرمين مستخدمي الانترنت بإمكانية الحصول على خدمات معينة تستوجب منهم الاشتراك مسبقا عن طريق دفع مبالغ زهيدة عبر موقع معين؛ فيقوم

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

…/……

الضحايا بالاشتراك لكن لا يحصلون على الخدمة، ورغم ذلك فإنهم لا يكترثون بمواجهة هذه الجريمة ولو عن طريق الاحتجاج وقد يعود السبب في ذلك إلى أن المبلغ المفقود لا يستحق الاحتجاج أو التبليغ لأنه في نظرهم يعد من قبيل الخسارة بالصدفة، لكن في حقيقة الأمر أن الجناة يحصلون على مبالغ كبيرة قد تصل بهم إلى حد الثراء مقارنة بعدد الضحايا الذين انطلت عليهم الخدعة الإجرامية[1].

الفرع الثاني: جرائم اختلاس أموال البنوك

لقد شهدت هذه الظاهرة تزايدا ملحوظا حتى أصبحت تؤرق أكثر الدول تقدما كالولايات المتحدة الأمريكية لتهديد أمنها القومي، كما سببت جرائم السطو الإلكتروني خسائر مالية كبيرة في أسواق المال الكبرى مما دفع الحكومات المختلفة إلى البحث عن وسائل مكافحة السرقة عبر الانترنت وحماية المستهلك ووضع أنظمة مختلفة لحماية تلك الأجهزة وكذلك عقد الاتفاقيات الدولية للحد من ظاهرة السرقة الإلكترونية[2].

وتعد قضية بنك الباسفيك الوطني الأمريكي مثالا حيا لهذا النوع من الجرائم، حيث اكتشف محاسبا مختصا في هذا البنك بالصدفة شفرة تحويل حسابات العملاء بين البنك وغيره من البنوك التي تتعامل معه، فقام بإصدار أوامر إلكترونية لعدة فروع تابعة للبنك بتحويل مبالغ قدرت جملتها بأربعة ملايين دولار لحسابه الذي فتحه في أحد المصارف السويسرية، ومرت شهور دون أن يكتشف أحد حقيقة ما حدث لولا اعتراف المتهم بالواقعة وهو سكران[3]. وفي نفس السياق ضبطت في فرنسا عمليات سطو بنكية عن طريق شبكة الانترنت شملت حوالي ثلاثين مليون حساب بنكي[4].

الفرع الثالث: جريمة الاختلاس عن طريق المزادات الوهمية.

المزاد الإلكتروني، هو مزاد يقام في فضاء الانترنت سواء كانت المواقع عامة أو خاصة، حيث يتم فيها عمليات بيع وشراء السلع عن طريق المزايدة في الثمن من قبل المشترين ويفوز بالصفقة من

---

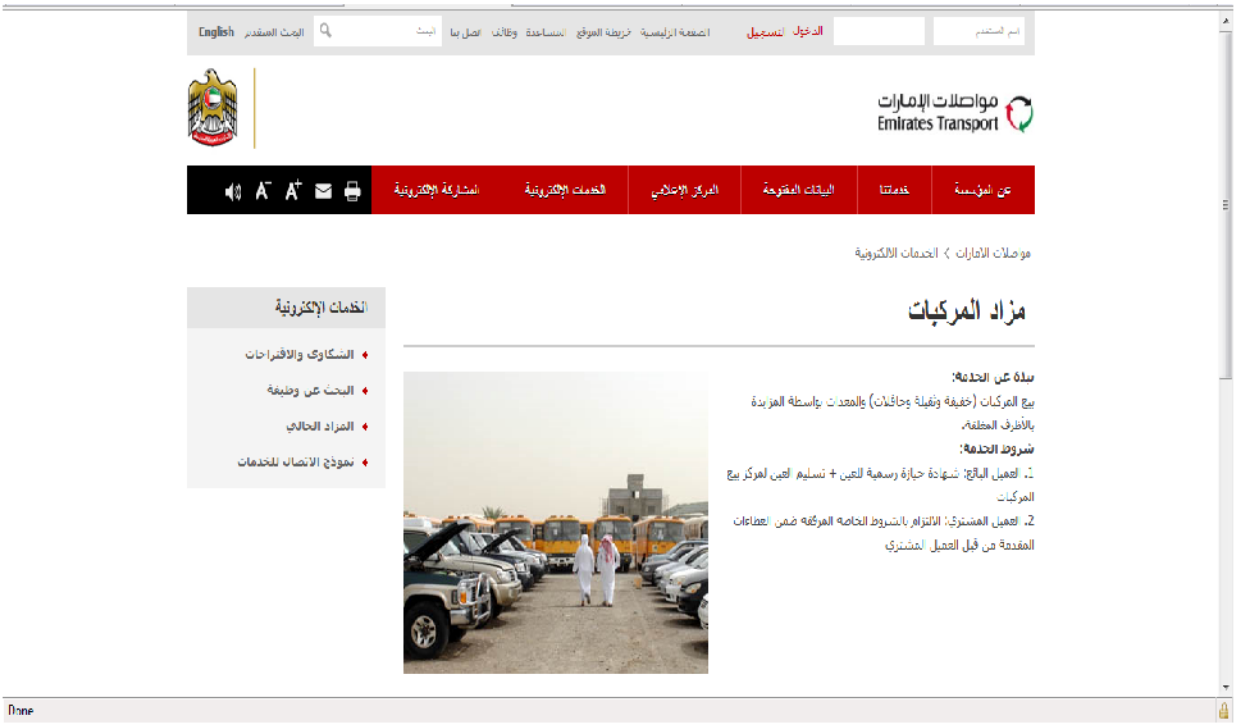
(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

يدفع أكثر، وبالمقابل تجني الأموال مواقع المزادات الالكترونية عن طريق الرسوم المخصومة من البائعين أو المشترين أو منهما معاً.

ويعود تاريخ ظهور المزاد الإلكتروني إلى سنة 1995م، ورغم حداثته فإن حجم المبيعات فيه يصل إلى مليارات الدولارات عالمياً، كما تتسم المزادات الإلكترونية بمجموعة من الخصائص كانخفاض تكلفتها واعتبارها أداة تسعير مرنة لم يكن يحلم بها التجار أو المستهلكين من ذي قبل بخلاف المزادات التقليدية التي كانت تعاني من ارتفاع تكاليفها وقلة المشاركة ومحدودية وقتها، ففي المزاد الإلكتروني بإمكان البائع أن يبيع لأكبر عدد من العملاء ويجني ربحاً أكثر دون إشراك الوسطاء، كما يستطيع بيع كميات كبيرة من المنتجات في وقت قياسي مقارنة بالمزادات التقليدية، أما المشتري فأصبح يملك خيارات أكثر من ذي قبل سواء على مستوى المنتجات أو أنواع المزادات كما لا يتكبد عناء وتكاليف التنقل من مزاد لآخر[1].



شكل رقم(15): يظهر أحد مواقع المزاد الإلكتروني في دولة الإمارات العربية المتحدة[2]

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

ولكون السلع المعروضة على مواقع المزادات هي في الحقيقة صور افتراضية للسلع محل التعاقد، فقد سهل استغلالها من طرف مجرمي الانترنت بالاحتيال على الغير وهو ما أكدته إحصائيات لجنة التجارة الفيدرالية Federal Trade Commission ولجنة مراقبة النصب عبر الانترنت Watch Internet Fraud بأن جريمة الاحتيال عن طريق المزادات الإلكترونية تعد الأكثر انتشارا في العالم الافتراضي[1]، حيث تعرض المواقع الوهمية على مستخدمي الانترنت منتجات بأسعار منخفضة جدا، وبمجرد أن يقرر مشاهدو هذه المنتجات شراءها يقومون بإرسال أرقام بطاقات الائتمان أو شيكات مصرفية لتحويل ثمن السلع إلى عنوان الموقع، فإن هذه المواقع تختفي مباشرة بعد حصولها على المال [2].

الفرع الرابع: جريمة اختلاس المال باستخدام بطاقات الائتمان

لقد أصبحت بطاقات الائتمان في ظل اندفاع العالم بقوة نحو المعلوماتية والتطور الإلكتروني الوسيلة الأكثر تداولا وقبولا في العالم خاصة في مجال التجارة الإلكترونية، كما بدأت بطاقات الدفع الإلكتروني تحل محل النقود والشيكات وتستخدم على نطاق واسع نظرا لما تتمتع به من سهولة الدفع وإمكانية التعامل بها محليا وعالميا، فضلا عن كونها ذات مسؤولية قانونية محدودة في حالة ما إذا تعرضت للضياع أو السرقة، الأمر الذي دعا البعض إلى اعتبارها جزءا لا يتجزأ من ثقافة النظام الاقتصادي العالمي المعاصر[3].

ولقد واكب انتشار بطاقة الائتمان وتزايد حجم التعامل بها نمو مطرد في الجرائم المصاحبة لاستخدامها؛ حيث احترف الكثير تزوير هذه البطاقات أو سرقتها واستخدامها في الاستيلاء على مال الغير وهذا راجع إلى سهولة تزوير بطاقات الائتمان من ناحية، وعدم توفر آلية عالمية لإحكام السيطرة على ضمان سرية بيانات هذه البطاقة من ناحية ثانية، إضافة إلى صعوبة إثبات التلاعب فيها من ناحية أخرى، وبذلك استطاع لصوص بطاقات الائتمان سرقة مئات الآلاف من بيانات البطاقات في يوم واحد من خلال شبكة الإنترنت ومن ثم استغلالها في شراء السلع حيث تم تحصيل القيمة من حساب الحاملين الشرعيين للبطاقات المسروقة، وفي حالات أخرى بيعت معلوماتها للغير بقصد الاستيلاء غير

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المشروع على الأموال[1] ونظرا لأهمية بطاقات الائتمان باعتبارها الوسيلة الأكثر تداولا في العالم فإنه يتعين علينا معرفة مفهومها وصور جرائم الاختلاس التي تطالها وذلك كما يلي: .

أولا: مفهوم بطاقة الائتمان من حيث الشكل والاصطلاح القانوني

من الناحية الشكلية تعرّف بطاقة الائتمان بأنها: "قطعة من البلاستيك بأبعاد قياسية معينة، مدونة عليها بيانات مرئية وأخرى غير مرئية، ويقترن إصدار البطاقة لحاملها بمنحه رقما سريا يعمل حال استخدامه للبطاقة في الوسط الإلكتروني، وهي تصدر عن منظمات أو بنوك تعتمد جانب الثقة في تعاملات العملاء، وبموجبها يمكن الشراء والدفع وسحب الأموال والحصول على الخدمات بأنواعها"[2].

شكل (16): نموذج لأحد بطاقات الائتمان المتعامل بها وبياناتها

وفي الاصطلاح القانوني تعرّف بطاقة الائتمان؛ "بأنها أداة مصرفية للوفاء بالالتزام، وهي مقبولة الدفع على نطاق واسع محليا ودوليا، كما تعد بديلا للنقود في دفع قيمة السلع والخدمات المقدمة لحامل البطاقة مقابل التوقيع على إيصال بقيمة الالتزام الناشئ عن شراء السلعة أو الحصول على

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

الخدمة، على أن يقوم التاجر بتحصيل القيمة عن طريق البنك المصدر للبطاقة والمصرح بقبولها كوسيلة دفع، ويطلق على هذا النوع من عمليات التسوية بنظام الدفع الإلكتروني الذي تغذيه الهيئات الدولية المصدرة للبطاقة"[1].

ومن بين التعريفات القانونية لبطاقة الائتمان أنها: "عقد بمقتضاه يتعهد مصدر البطاقة بفتح حساب بمبلغ معين لمصلحة شخص آخر هو حامل البطاقة، الذي يستطيع بواسطتها الوفاء بمشترياته لدى المحلات التجارية التي ترتبط مع مصدر البطاقة بعقد تتعهد فيه بقبولها الوفاء بمتطلبات حاملي البطاقات الصادرة عن الطرف الأول، على أن تتم التسوية النهائية بعد كل دورة محددة"[2].

ثانيا: صور اختلاس المال عن طريق بطاقات الائتمان.

1 ــ احتيال الحامل الشرعي لبطاقة الائتمان:

ويقصد بالحامل الشرعي هنا؛ صاحب البطاقة الأصلي المخول له استخدامها كوسيلة دفع للحصول على السلع والخدمات المختلفة، وغالبا ما تتخذ جرائم العميل إحدى الصور التالية:

ــ استصدار بطاقة ائتمان صحيحة بناء على مستندات مزورة: فهناك من المحتالين من يتقدم إلى البنوك بمستندات إثبات شخصية مزورة، للحصول على بطاقات ائتمان بأسماء منتحلة وعناوين أو ضمانات وهمية، حيث تستخدم هذه البطاقات في شراء سلع بمبالغ كبيرة، وبالتالي يعجز البنك عن مطالبة حامل البطاقة بقيمة المشتريات، إما لعدم إمكانية الاستدلال عليه، أو لعدم وجود ضمانات تكفي لاسترجاع قيمة ما دفعه البنك للتاجر.

ــ التجاوز المتعمد لحد السحب بالتواطؤ مع موظفي البنك خاصة في مجال التجارة الإلكترونية.

ــ تواطؤ العميل مع الغير بإعطائهم رقم استعمال البطاقة لاستخدامها في دول أخرى، ثم يقوم بالاعتراض على الخصم من حسابه، على أساس أنه لم يغادر البلاد و لم يستخدم البطاقة.

ــ استخدام خدمات نقاط البيع الإلكترونية في إيداع شيكات بدون رصيد، بحيث تضاف قيمة الشيك إلى قيمة الحسابات الأصلية، ثم يقوم العميل بسحب المبالغ المضافة بواسطة نقطة البيع

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الإلكترونية قبل إجراء المقاصة بين البنوك[1].

ـــ تواطؤ العميل مع التاجر، حيث يقوم الحامل الشرعي للبطاقة باستخدامها بعد استنفاد رصيدها الشهري في إجراء عمليات شراء بالاتفاق مع التاجر، وبذلك يحصل العميل على نسبة نقدية من قيمة الفاتورة، بينما يحصل التاجر على باقي المبلغ نظير إتمام تلك العمليات، وتحصيل قيمة هذه الفواتير من البنك.

ـــ سحب العميل لكامل رصيد البطاقة، ثم الإبلاغ عن ضياعها قبل زمن السحب. [2]

2ـــ احتيال موظفي البنك المصدّر لبطاقة الائتمان:

لقد تم تسجيل العديد من التجاوزات الخطيرة التي تصدر من موظفي البنوك مصدّرة بطاقات الائتمان عن طريق الاستخدام غير المشروع لها، وغالبا ما تتخذ أساليب الاحتيال التي تقع من موظفي البنك أحد الصور التالية:

ـــ استغلالا لعدم دراية العميل الكافية بأنظمة البطاقة، يتم التلاعب في رصيدها من خلال حركات الإيداع والسحب الالكتروني لصالح الموظف.

ـــ يتواطأ موظف البنك مع العميل صاحب البطاقة في استخراج بطاقة سليمة ببيانات مزورة، وأحيانا يسمح للعميل بتجاوز حد البطاقة في السحب، كما يسمح للعميل بالصرف بموجب بطاقة منتهية الصلاحية أو عثر عليها.

ـــ تواطؤ موظف البنك مع التاجر في تجاوز حد السحب في صرف قيمة الإشعارات، أو اعتماد إشعارات مستندة إلى بطاقات وهمية أو مزورة أو منتهية الصلاحية أو مسحوبة.

ـــ تواطؤ موظف البنك مع بعض المجرمين بمدهم ببيانات تخص بطاقات الوفاء أو السحب الصحيحة المتداولة للاستيلاء على أرصدتها، وعادة ما يتم التركيز على البطاقات ذات سقف الائتمان المرتفع كالبطاقات الذهبية Gold Cards وعلى أفراد ذوي سمعة تجارية عريقة[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

3 ــ احتيال التاجر عن طريق بطاقات الائتمان:

ينصرف مفهوم التاجر هنا إلى جميع الجهات التي تقبل البطاقات من حامليها كوسيلة دفع الكترونية مقابل السلع والخدمات المقدمة، كالمحال التجارية، والفنادق، والمطاعم وغيرها.. حيث يحل التاجر محل البنك في تأدية الخدمة لحامل البطاقة عن طريق استخدام الأدوات البنكية المسلمة إليه لإتمام عمليات الشراء، وبذلك يكون المجال واسعا أمام التاجر في النصب والاحتيال من خلال الآليات المتاحة بين يديه[1].

ومن أبرز صور الاحتيال التي يقوم بها التاجر باستغلاله لبطاقة الائتمان:

ــ يشتري بعض التجار إشعارات بيع من الغير مطبوع عليها أرقام بطاقات عملاء مزورة أو صحيحة لأنها حررت على غرار بيانات بطاقات فعلية، ثم يقومون بطباعة رقم آلاتهم الخاصة بعمليات الشراء حتى يتمكنوا من تحصيل قيمة الإشعارات على الرغم من عدم قيامهم بأي خدمة فعلية، مما يترتب عليه اعتراض الحامل الشرعي للبطاقة الأصلية التي اختلست بياناتها[2].

ــ يقوم بعض التجار بطباعة أرقام بطاقات العملاء المتعاملين معهم على إشعارات فارغة دون طباعة رقم آلتهم وبيعها لتجار آخرين ليحصلوا على قيمتها [3].

ــ قيام بعض التجار بشراء بطاقات مسروقة واستخدامها في عمليات بيع وهمية وتحصيل قيمتها من البنك بالتحايل[4].

ــ تزوير توقيعات العملاء على فواتير لمشتريات لم يحصلوا عليها، وتحصيل قيمتها من البنك الذي يتولى خصمها من حاملي البطاقات[5].

ــ كما يحتال التاجر على أصحاب البطاقات خاصة الأجانب منهم بالزيادة في المبالغ الأصلية على إشعارات البيع مغافلة لحامل البطاقة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

4 ــ احتيال غير المالكين الأصليين لبطاقات الائتمان:

يعتبر تزوير بطاقات الائتمان في نطاق شبكة الانترنت من أخطر وأدق طرق الغش في مجال معالجة البيانات بطريقة آلية لاسيما بعد حلول المستندات الالكترونية محل الأوراق التقليدية وهو ما زاد من صعوبة اكتشاف الجريمة أو إثباتها، وغالبا ما يتخذ الاحتيال في هذه الحالة الأشكال التالية:

ــ الاحتيال باستخدام بطاقات الدفع المزورة، حيث يقوم الجاني بإيهام التاجر بأنه الحامل الشرعي للبطاقة بعدما يقدم له أوراق ومستندات منسوبة للغير مع بطاقة تم تزويرها وفق المستندات المرفقة والبيانات المحصلة منتحلا بذلك شخصية صاحب المستندات الأصلي فيحصل الجاني من التاجر على ما يريد من السلع والخدمات.

ــ تواطؤ الحامل الشرعي للبطاقة مع الغير، كأن يعطي حامل البطاقة الأصلي للغير بطاقته ليستخدمها بدلا عنه في السحب ثم يبادر بالاعتراض على هذه العمليات كما يطعن بالتزوير على توقيعه، وبعدما يثبت التزوير يتحمل مصدر البطاقة خسارة الأموال المسحوبة من قبل الغير[1].

ــ سرقة بيانات البطاقة الائتمانية، يثير استعمال البطاقات الإلكترونية على شبكة الانترنت مشاكل كبيرة لأن التعامل بها في ساحة الانترنت يكون عبر فضاء مفتوح مما يجعل مستعمل البطاقة عرضة لمئات الآلاف ممن يحاولون اصطياد بياناتها وأرقامها بهدف الاستيلاء على رصيده المالي.

فآلية الشراء عبر شبكة الانترنت باستخدام البطاقة الائتمانية تعتمد على تزويد التاجر برقم البطاقة الخاصة بالعميل والعنوان الذي يرغب باستلام السلعة من خلاله ومعلومات شخصية أخرى كي يصل الطلب خلال الفترة الزمنية المتفق عليها، وفي الوقت الذي تتولى فيه شبكات البنوك العالمية والشركات إجراء عمليات المقاصة بين الحسابات وتقييد الفوائد والعمولات وفقا للاتفاقات والبروتوكولات المتعلقة بهذا الشأن[2]، فإن هذه الميزة الإيجابية لعملية الشراء الإلكتروني يقابلها الاستغلال غير المشروع لمواطن الضعف التي كشف عنها التطبيق العملي لهذا النظام، حيث تتعرض الأرقام والبيانات الخاصة بتلك البطاقات إلى الالتقاط غير المشروع من قبل الغير، وبالتالي الاعتداء

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

على الذمة المالية لصاحب البطاقة أو البنك المصدّر لها، وهذا وفق أساليب عديدة يتبعها قراصنة بيانات البطاقات الائتمانية من أشهرها ما يلي:

ـــ الاختراق الغير مشروع لمنظومة خطوط الاتصالات العالمية Illegal access : وهو من أخطر الأساليب التي تهدد عملية التسوق عبر شبكة الانترنت، حيث يقوم المقتحم بتسخير كل خبراته وبرامجه لتجاوز جدار الحماية للملفات المتضمنة للمعلومات الشخصية للعملاء والمخزنة في الكمبيوتر الرئيسي عبر الشبكة العنكبوتية.

ـــ الاصطياد الالكتروني Phishing: وهو أسلوب يقوم على نسخ موقع من مصدر موثوق به كمصرف على سبيل المثال، ثم يقوم الجاني بإرسال وصلة إلى موقع إلكتروني آخر مخادع يطلب فيه بعض المعلومات المهمة كالاسم ورقم الحساب المصرفي والرقم القومي واسم المستخدم وكلمة المرور المتعلقة بالمستهلكين، وبعد الاستجابة يتم استخدام تلك المعلومات في تحويل المال إلى حسابات الجناة المصرفية أو يتم الاستهلاك غير المشروع لأموال الغير عن طريق شراء سلع ثمينة كالمجوهرات والمواد الإلكترونية[1].

ـــ تقنية تفجير الموقع المستهدف، وهو أسلوب يوجه إلى الحواسيب المركزية (خادم الانترنت) الخاص بالبنوك والمؤسسات المالية، والمطاعم، والفنادق، ووكالات السفر بهدف الحصول على أكبر قدر ممكن من أرقام البطاقات الائتمانية، وذلك عن طريق ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز المجرم إلى الأجهزة المستهدفة، حيث يشكل هذا الكم الهائل من الرسائل ضغطا كبيرا على الأجهزة المستهدفة مما يؤدي إلى تفجير الموقع العامل على الشبكة وبالتالي تتشتت المعلومات والبيانات المخزنة فيه، الأمر الذي يفتح المجال للمجرم بحرية الدخول في الموقع المستهدف بسهولة وبالتالي يحصل على كل ما يحتاجه من أرقام ومعلومات وبيانات بطاقات الائتمان الخاصة بالعملاء.

ـــ أسلوب الخداع، يقوم فيه المجرم بإنشاء مواقع وهمية على شبكة الانترنت على غرار مواقع الشركات والمؤسسات التجارية الأصلية التي توجد على الشبكة ويظهر وكأنه الموقع الأصلي مقدم الخدمة، وبذلك يستقبل الموقع الوهمي جميع المعاملات المالية والبنكية والتجارية التي يقدمها الموقع الأصلي عبر شبكة الانترنت لأغراض التجارة الإلكترونية التي تعتمد في أغلبها على البطاقات

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الائتمانية مما يستلزم الحصول على المعلومات الخاصة بها، كما يستقبل أيضا الموقع الوهمي كافة الرسائل الإلكترونية الخاصة بالموقع الأصلي فيتم الإطلاع عليها والاستفادة غير المشروعة من المعلومات الموجودة بها على نحو يضر بأصحاب المواقع الأصلية وهو ما يؤثر سلبا في موثوقية التجارة الإلكترونية والذي بدوره يؤدي إلى الإخلال باقتصاديات الدول.[1]

ـــ اعتماد المعادلات الرياضية والإحصائية، ويعرف هذا الأسلوب لدى مجرمي البطاقات بـــ "Card Math" حيث يعتمد فيه بالدرجة الأولى على إجراء معادلات رياضية وإحصائية بهدف تحصيل أرقام بطاقات ائتمانية مملوكة للغير[2]، وكمثال على ذلك فقد حصل أن طالبا جامعي بمدينة الإسكندرية ضبط بتهمة الاستيلاء على مبالغ طائلة من حسابات بعض البطاقات الائتمانية الخاصة بعملاء أحد البنوك بالجيزة عبر شبكة الانترنت واستخدمها في عمليات التسوق، وهذا بعدما تمكن من الحصول على أرقام تلك البطاقات باستخدام بعض المعادلات الحسابية الدقيقة[3]، علما أن نماذجا عديدة من هذه المعادلات وخطوات استعمالها للحصول على أرقام البطاقات الائتمانية المملوكة للغير منشورة على مواقع الانترنت، وهو ما زاد في حدة جرائم السطو على بطاقات الائتمان[4].

المطلب الثالث: جريمة غسيل الأموال الإلكترونية

يعد غسيل الأموال من أخطر الجرائم المالية التي يعاني منها العالم بالنظر إلى ما تلحقه من آثار سلبية في كافة المجالات الاقتصادية، والاجتماعية، والسياسية، والأخلاقية..، سواء على المستوى المحلي أو الإقليمي أو الدولي، و لم يتوان مجرمي غسيل الأموال من استغلال التطور الهائل الذي شهده قطاع الاتصالات وانتشار شبكة الانترنت واستخدام البنوك لنظام الحواسيب الالكترونية في تنفيذ جرائمهم بطرق أشد دقة وخطورة من الوسائل التقليدية السابقة، خاصة وأن التكنولوجيا الحديثة ألغت الحدود الجغرافية التي كانت تشكل أكبر عائق لهم في هذا النوع من الجرائم.

الفرع الأول: مفهوم جريمة غسيل الأموال في القانون الوضعي

عرف مصطلح غسيل الأموال في القانون الوضعي تعريفات عديدة أهمها:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

هي جميع العمليات والإجراءات المتخذة بغرض تغيير صفة الأموال المحصل عليها بطرق غير مشروعة لتبدو كما لو أنها مكتسبة من مصادر مشروعة، وذلك عن طريق إنشاء مشاريع وهمية، أو فتح حسابات وإيداع الأموال في البنوك التي لا يهمّها مصدرها كالبنوك المتواجدة بسويسرا وبَنَمَا وموناكو[1].

كما تعرّف جريمة غسيل الأموال على أنها: إخفاء وتمويه الطبيعة الحقيقية للأموال المكتسبة بطرق غير مشروعة بواسطة عمليات مادية وهمية بهدف منحها الوجه الشرعي، فهي جريمة تقوم على صناعة واقع زائف وجعله حقيقي[2].

وتتفق التشريعات القانونية في أغلبها على أن جريمة غسيل الأموال تقوم على أساس إخفاء كل مال ناشئ عن مصدر غير مشروع بدمجه في الدورة الاقتصادية المشروعة بغرض إخفاء مصادره الأصلية، وذلك اعتمادا على تنظيم مؤسسي يضم عددا من المحترفين يعملون وفق هيكلة بالغة الدقة والتعقيدات والسرية[3].

وتعرّف أيضا جريمة غسيل الأموال، بأنها إخفاء الرابطة بين المجرم والجريمة وذلك من خلال عمليات متعددة ترمي إلى تمويه أو طمس معالم المصدر الجرمي للأموال، وتحويلها من أصول نقدية إلى أصول حسابية بنكية سواء داخل الدولة أو خارجها بما يجعلها في مأمن من أجهزة تنفيذ القانون ويقلل من حجم المخاطر القانونية التي تواجه المجرمين من ناحية، وتمكنهم من التصرف بحرية في هذه الأموال من ناحية أخرى، كاستخدام عائدات الجرائم لتحقيق أهداف استثمارية بحتة، من خلال العمل في مشروعات قانونية والاندماج في الاقتصاد المشروع، وهو ما يوفر لغاسلي الأموال المرونة لتحقيق المزيد من الأرباح، وبلوغ المكانة الاجتماعية المرموقة[4].

الفرع الثاني: مفهوم جريمة غسيل الأموال الإلكترونية.

لقد ارتبط مفهوم جريمة غسيل الأموال الإلكترونية باستغلال التقنية الحديثة، حيث تعرّف بأنها كل العمليات التي يتم من خلالها استخدام نظم نقدية ومالية ذات تقنية متطورة لإضفاء صفة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المشروعية على الأموال المحصلة من مصادر غير مشروعة بواسطة الانترنت.[1]

فبعدما كانت المرحلة الأولى لغسيل الأموال التقليدية تعد بالنسبة للمجرمين من أصعب المراحل بالنظر إلى مخاطر اكتشاف الجريمة، فإن الأمر يختلف في غسيل الأموال الإلكتروني لما يتسم به من خاصية التشفير ذات السرية العالية وهو ما يسهل تخطي عقبة افتضاح الأمر، هذا بالإضافة إلى عدم خضوع العديد من المؤسسات المالية غير المصرفية للرقابة مما يسهل عمليات شراء النقود الإلكترونية[2] بواسطة البطاقات الذكية أو الحاسوب الشخصي، ولإضفاء صفة المشروعية على هذه الأموال يقوم غاسل الأموال بالعديد من العمليات من خلال الحاسوب الشخصي دون الحاجة لطرف وسيط خلافا للطرق التقليدية، كما ساعد أيضا لجوء الكثير من المصارف إلى تقديم خدماتهم المالية والمصرفية من خلال وسائل الكترونية حديثة تتزامن مع التطورات التكنولوجية، الأمر الذي مكن غاسلي الأموال في الاستفادة من هذه التقنيات وتطوير أساليب غسيل الأموال بتخليهم قدر الإمكان عن الأساليب التقليدية لتفادي الرقابة المصرفية واستحالة تتبع مصادر الأموال غير المشروعة[3]، ومن بين هذه الأساليب ما يلي:

1 ـــ تقنية موندكس في غسيل الأموال Mondex :

هي تقنية يتمكن من خلالها تحويل الأموال غير المشروعة عبر الانترنت مع ضمان تشفير آمن لهذه العمليات بدون ترك أي أثر يدل على الجريمة. وتتميز هذه التقنية في غسيل الأموال بابتعادها عن القطاع المصرفي الحكومي أو الخدمات المصرفية التقليدية إضافة إلى سهولة تجاوزها للحدود، مما يجعل عملية تتبعها أمرا مستحيلا، ولقد شكلت هذه التقنية عائقا كبيرا في التشريعات التقليدية التي استوجب إعادة النظر فيها لمواكبة التطورات التكنولوجية الحديثة قصد مواجهة هذه الظاهرة[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ــ بنوك الانترنت Internet Banking :

تتيح الانترنت لكل فرد إمكانية إنشاء بنك أو متجر افتراضي أو صرافة للعملة أو شركات وهمية في البلدان التي تغض النظر عن عمليات غسيل الأموال، حيث تتداول فيها النقود الإلكترونية كعملة أساسية وهو ما يصعب مهمة رقابة وسيطرة الجهات الحكومية التنفيذية واختصاص تشريعاتها القانونية الخاصة بالعمليات المصرفية، ولذلك تعد بنوك الانترنت هي الوسيلة المثلى في تسهيل عمليات غسيل الأموال لكونها شخصيات افتراضية لا تخضع لرقابة التشريعات والقوانين المتعلقة بالبنوك التجارية الاعتيادية التي تخضع لرقابة البنوك المركزية، إضافة إلى وجودها خارج نطاق الاختصاص المكاني والتشريعي الذي يعطي البنوك المركزية سلطة الرقابة المصرفية عليها وتنظيم أنشطتها وحق ملاحقتها عند ارتكاب أية مخالفات قانونية.[1]

3 ــ النقود الإلكترونية Electronic money :

تؤدي النقود الإلكترونية دور هاما في تنشيط الحياة الاقتصادية خاصة في الدول المتقدمة لأنها تمكن المتعاملين بها من إتمام صفقاتهم من أي مكان يتواجدون فيه، لكن لم يخلو هذا النوع من النقود من سلبيات خطيرة كعلاقتها بجريمة غسيل الأموال، حيث تسهل ارتكاب هذه الجريمة بسبب استحالة تعقبها، وسرعة حركتها، وعدم خضوعها للاختصاص التشريعي المصرفي للدول باعتبار غياب الفضاء المادي التقليدي الذي يحددها، مما يمكن تحويل الأموال بحرية دون عوائق ودون الحاجة إلى خدمات البنوك والوسطاء الماليين، وهو ما يجعلها خارج سلطات الرقابة المصرفية[2]، خاصة وأن النقود الإلكترونية لا تخضع لمعايير النقود القانونية التقليدية التي تفرض على الدول المصدرة لها وجوب توفر غطاء قانوني واحتياطي إجباري يتناسب مع مقدار النقود المصدرة، وهو أيضا ما جعل النقود الإلكترونية خارجة عن اختصاص البنوك المركزية.

4 ــ بطاقات الائتمان Credit Cards :

تستخدم أيضا بطاقات الائتمان في عمليات غسيل الأموال بالنظر إلى خاصيتها في نقل الأموال

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المشحونة على البطاقة إلى أي مكان في العالم، بالإضافة إلى ما توفره من إمكانية استيعاب أموالا إضافية عليها، كما يمكن استخدامها كأحد وسائل الدفع في دول عديدة دون الحاجة إلى تحمل مخاطر حيازة النقود، حيث تودع أموالا طائلة في حساب البطاقة وتمكن المبيض من سحبها أينما وجد في العالم.[1]

5 ــ نوادي القمار الإفتراضية Virtual Casions :

هي مواقع افتراضية توفر كل أنواع القمار وألعابه يديرها أشخاص من منازلهم أو مكاتبهم، وتساهم هذه النوادي الافتراضية بشكل كبير في عمليات غسيل الأموال نظرا لصعوبة تتبع أماكن تواجدها الفعلي، إضافة إلى خروجها عن نطاق الاختصاص المكاني لدول معينة، حيث يلجأ غاسلي الأموال إلى هذه النوادي الافتراضية بشرائهم لما يسمى بالفيش وقسائم اللعب مقابل أموال نقدية، وبعد ذلك يتم استبدال الفيش بشيكات مسحوبة على مصارف معينة، لتظهر وكأنها أموال ناتجة عن ربح من ألعاب القمار[2].

الفرع الثالث: الآثار السلبية لجريمة غسيل الأموال.

تنعكس سلبا آثار جريمة غسيل الأموال على كل من الحياة الاقتصادية، والسياسية، والأمنية، والاجتماعية وذلك كما يلي:

أولا ــ آثار غسيل الأموال على الاقتصاد القومي:

في الغالب يقوم أصحاب غسيل الأموال بتبييض أموالهم في البلدان النامية حيث لا تزال فيها وسائل الرقابة ضعيفة مما يسهل اختراق القوانين والتشريعات المتعلقة بالأموال، ويختارون في العادة البلدان التي تتميز بمعدلات فائدة قليلة وعدم الاستقرار في أسعار الصرف، فيؤدي غسيل الأموال بها إلى بروز مؤشرات اقتصادية مضللة خاصة ما يتعلق بمعدلات الفائدة وأسعار الصرف والمالية العامة، كما أن انتقال هذه الأموال في ظل العولمة من اقتصاد لآخر يمكن أن يؤدي إلى عدم الاستقرار الاقتصادي حتى على المستوى الدولي.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما يؤدي غسيل الأموال إلى إعادة توزيع الدخل، عن طريق بروز مستثمرين جدد يتمتعون بقدرات كبيرة في مجالي الادخار والاستثمار مما ينعكس سلبا على كبار رجال الأعمال والمستثمرين العدول من جهة، وعلى النمو الاقتصادي من جهة أخرى، هذا بالإضافة إلى احتمال تفشي الاحتيال والاختلاس في الأسواق والمشروعات المربحة وسريعة النمو، كما تؤثر عمليات غسيل الأموال على دخل فئات المجتمع، إذ تتحول مداخيل الفئات المنتجة التي تحقق دخلا مشروعا إلى فئات غير منتجة نتيجة حصولها على مداخيل غير مشروعة مما يزيد الفجوة بين الأغنياء والفقراء فيتضاعف الخلل الاجتماعي في البلد المتضرر[1].

و من الآثار السلبية أيضا لغسيل الأموال أنه يؤدي إلى تعطيل تنفيذ السياسات المالية العامة عن طريق التهرب الضريبي، مما ينعكس سلبا على ميزان المالية العامة وبالتالي على موارد الحكومة المتاحة لمقابلة التزاماتها وعلى أدائها الاقتصادي والاجتماعي.

ثانيا ــ آثار غسيل الأموال على الحياة الاجتماعية:

يظهر أثر غسيل الأموال على النواحي الاجتماعية من خلال قلة الموارد واستنزاف المداخيل؛ وهو ما يؤدي إلى حرمان الطبقات الفقيرة من الخدمات الضرورية كالصحة، والتعليم، والإسكان لكون هذه الخدمات تحتاج إلى تمويل من الدولة، وعلى الجانب الآخر فإن الفئات الأخرى تستطيع شراء هذه الخدمات بما لديها من مداخيل عالية، ومن هنا تظهر الطبقية بين الأغنياء والفقراء الأمر الذي ينتج عنه كثرة الجرائم في المجتمع ويضعّف البلد، وتنعدم القيم والأخلاق والروابط الاجتماعية بين الأفراد، كما ينتج أيضا عن الفجوة بين طبقة الأغنياء والفقراء تحدي النظام والتمرد عليه بسبب الإحساس بعدم التوازن الاجتماعي والاقتصادي فينتشر الفساد وتضعف الثقة بين الناس، وينتج عن ذلك اختلال الهيكل الاجتماعي وتزايد حدة الفقر بسبب التفاوت في توزيع الموارد وتدني مستويات المعيشة للغالبية العظمى من المجتمع[2].

ثالثا ــ آثار غسيل الأموال على الحياة السياسية والأمنية:

لقد أثبتت الدراسات بوجود علاقة بين غسيل الأموال والاضطرابات الاجتماعية والسياسية؛

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كحركات الإرهاب والتطرف والعنف الداخلي، فضلا عن نشاط المافيا العالمية ودورها في حدوث الانقلابات السياسية في بعض الدول النامية مما يزعزع أمن واستقرار المجتمعات النامية في دول العالم الثالث، كما تستعمل عمليات غسيل الأموال في توفير الدعم المالي وتمويل شراء الأسلحة لتغذية الانقلابات العسكرية والسياسية على مستوى العالم وذلك بالتعاون مع أجهزة متخصصة في تنظيم وإدارة الصراعات السياسية والإستراتيجية عالميا.

كما أثبتت دراسات متخصصة وجود علاقة وثيقة بين الجوسسة السياسية والاقتصادية وبين غسيل الأموال، إذ تحتاج أجهزة الجوسسة إلى التمويل اللازم لعملياتها حول العالم فتتجه إلى استخدام البنوك التجارية وفروعها ومراسليها في العديد من الدول لتوجيه الأموال إلى مزاولة العمليات التجسسية في مختلف أنحاء العالم. كما تلجأ بعض أجهزة التجسس إلى استخدام غسيل الأموال في تأسيس شركات وهمية لمزاولة الأعمال غير المشروعة وتدبير الانقلابات، وتنفيذ بعض العمليات التخريبية الموجهة إلى أنظمة أو حكومات معينة في مختلف الدول، كما تستخدم بعض الأحزاب والفرق السياسية حصيلة أموال تجارة المخدرات، وتزييف النقد المحلي والأجنبي في تمويل عملياتها العسكرية ضد نظام الحكم تحت غطاء الصراع على السلطة السياسية كما هو الحال في عدد من الدول التي اشتهرت بزراعة وتجارة المخدرات. [1]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني:
الجرائم الإلكترونية المتعلقة بالأشخاص والآداب العامة

في كثير من الأحيان يتعرض مستخدمي الانترنت لانتهاك خصوصياتهم الفردية إما عمدا أو مصادفة، ويعود السبب في ذلك إلى الثغرات التقنية الحاصلة أثناء الإبحار في الانترنت، فعلى سبيل المثال ما إن يزور مستخدم الانترنت موقعا معينا على الشبكة حتى يقوم ذلك الموقع تلقائيا بإصدار نسختين مما يسمى بالكعكة الخاصة Cookies، وهي عبارة عن معلومات صغيرة ترسلها مواقع الويب لتخزينها في أجهزة الزائرين لأهداف متعددة كالتعرف على من يكرر زيارة الموقع مثلا، حيث تبقى نسخة منها في الجهاز الخادم (SERVER) الخاص بالموقع والنسخة الأخرى يتم تخزينها تلقائيا على القرص الصلب لجهاز الزائر دون علمه، وينتج عن هذه الكعكة إصدار رقم خاص يميز كل زائر عن غيره من الزوار حيث تبدأ بجمع المعلومات وإرسالها إلى مصدرها أو إلى إحدى شركات الجمع والتحليل للمعلومات والتي في الغالب ما تكون أهدافها دعائية، لكن قد تستغل بعض المواقع المشبوهة هذه المعلومات عن طريق نسخها والاستفادة منها بطرق غير مشروعة للاعتداء على الأشخاص.[1]

المطلب الأول: صور الجرائم الإلكترونية المتعلقة بالأشخاص

الفرع الأول: التشهير الإلكتروني

التشهير هو كل العبارات العلنية سواء كانت شفهية أو كتابية التي من شأنها أن تسيء إلى سمعة الشخص أو اسمه أو تحط من منزلته في نظر معارفه أو المجتمع ككل.

أولا ــ صور التشهير الإلكتروني وآثاره.

إن المتأمل في واقع الانترنت يجد أن مسألة التشهير بالأشخاص من أبرز الأمور تداولا خاصة على مواقع الحوارات والنقاش، كما صممت العديد من المواقع الالكترونية خصيصا لأجل التشهير بالأشخاص وهي مواقع يرتادها الكثير من الناس من باب التفكه بذكر عيوب الغير والتشهير بهم عبر إيراد معلومات سرية أو مغلوطة أو مضللة، وقد يكون الضحية فردا أو مجتمع أو مؤسسة تجارية أو هيئة سياسية، ولقد رصدت المصادر الإخبارية الإلكترونية منها والورقية مئات الآلاف من الحالات

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

التي تبرز فيها مدى تضرر الضحايا من هذه الجرائم وما نتج عنه من فقدان وظائفهم وتشتت أسرهم وأبنائهم، وقد لجأ الضحايا في بعض الأحيان إلى الانتحار هروبا من فضيحة التشهير ونظرة المجتمع لهم المشبعة بالظنون.

ولقد تسللت ظاهرة الابتزاز والتهديد بالتشهير عن طريق نشر صور محرفة إلى وسط المدارس، وأصبحت لعبة في أيدي التلاميذ يوجهونها بدون وعي كامل بالنتائج الوخيمة المترتبة عنها، خاصة إذا وجهت للشخص الخطأ كما وقع مع تلميذه تدعى "تقوى" التي انساقت وراء التهديدات العابثة لبعض التلاميذ بعرض صور مفبركة لها على مواقع التواصل الاجتماعي، وكان الاستسلام للموت انتحارا خيار هذه الضحية، علما أن اختيار الانتحار لمواجهة طوفان التهديدات بالتشهير والابتزاز لم يكن خيارا منفردا لهذه الضحية، حيث أكدت العديد من الوقائع الأخيرة أن ضحايا الانتحار تعرضوا لضغوطات كبيرة قبيل هلاكهم، ونسبة كبيرة منهم كانوا ضحية الابتزاز والتهديد بالتشهير بصور خصوصية إما واقعية أو مفبركة فاضحة..[1]

ثانيا ــ أسباب ودوافع انتشار ظاهرة التشهير الإلكتروني.

قد تكون أهم أسباب انتشار هذه الظاهرة على الإنترنت هو سهولة نشر المعلومات ووصولها إلى أعداد كبيرة من الناس مع صعوبة التعرف على ناشر المعلومة أو منعه من نشرها، وحتى في حال معرفة الناشر فإن عالمية الإنترنت تجعل من الصعب محاكمته، لاختلاف قوانين الدول، وتعدد الأماكن التي يحصل فيها التشهير، ولذلك يمكن حصر سببين رئيسين للظاهرة هما:

1 ــ أن مرتكبي هذا التصرف المشين يختفون وراء أسماء وهمية فيأمنون بذلك من العقوبة حسب زعمهم.

2 ــ أن المتعاملين بالانترنت لا تحدهم حدود جغرافية، فتجد المشهر بالغير من بلد والمشهر به في بلد آخر، الأمر الذي يأمن معه من الملاحقة القضائية أو ردة فعل الضحية.

أما دوافع التشهير فمعظمها مرتبط بما يلي:

ــ الكيد والحسد للمُشهر به من أجل التقليل من مكانته.

ــ العداوة للمشهر به نتيجة خلاف ما، فيبدأ أحدهما بوصف الآخر بصفات قبيحة وألفاظ نابية.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ التلذذ بوصم الآخر بكل عيب ليحط من مترلته في المجتمع حتى ولو لم تكن بينهما معرفة أو معاملة.

ـــ المخالفة في الفكر؛ كأن يختلف اثنان في اتجاه ما فينعت أحدهما الآخر بأنه مبتدع أو زنديق، أوعلماني، أو متطرف ليقلل من مكانته في المجتمع حتى لا يُسمع له، وهو ما يحدث غالبا في الطبقة المثقفة.[1]

الفرع الثاني: جريمة القذف والشتم.

أولا ـــ مفهوم القذف

القذف في اللغة: الرمي بالحجارة، يقال قذف بالحجر وبالشيء قذفا رمى به بقوة، ويقال قذفه بالكذب: نسبه إليه، وقذف بالحق على الباطل أي رماه فأبطله[2]، قال تعالى: ﴿بَلْ نَقْذِفُ بِٱلْحَقِّ عَلَى ٱلْبَٰطِلِ فَيَدْمَغُهُۥ فَإِذَا هُوَ زَاهِقٌ﴾[3].

والقذف في الاصطلاح الفقهي هو: الرمي بالزنا[4]، وزاد الشافعية[5]: في معرض التعيير، وعرفه المالكية[6] بأنه: رمي مكلف حرا مسلما بنفي نسب عن أب أو جد أو بزنا.

أما القذف في الاصطلاح القانوني فهو إسناد مادة معينة إلى شخص ولو في معرض الشك والاستفهام، ومن شأنها أن تنال من شرفه وكرامته، أو تعرّضه للاحتقار عند الناس، سواء كانت تلك المادة جريمة تستلزم العقاب أم لا.[7]

ثانيا ـــ دوافع جرائم القذف والشتم وصورها

في الغالب تهدف جرائم القذف والشتم الالكتروني إلى المساس بشرف الغير أو كرامتهم واعتبارهم، وقد يحصل القذف والسب عن طريق الاتصال المباشر بالضحية أو يكون كتابيا كأن يحرر على شكل رسائل قصيرة موجهة إلى هاتف الضحية، أو يكون عن طريق شبكة الانترنت باستعمال

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

صفحات الويب أو غرف المحادثة، أو البريد الإلكتروني[1]، و يتخذ الجاني هذه الوسائل الإلكترونية لإيصال عبارات السب والقذف إلى أكبر عدد ممكن من الأفراد وبذلك يتحقق ركن العلنية باعتبار شبكة الانترنت مسرحا غير محدود، فهي تتلقى كل ما يدرج فيها دون قيد أو رقابة ولذلك فإن استخدامها السلبي حتما سيلحق أضرارا جسيمة بالغير.[2]

الفرع الثالث: جرائم التعدي على الحياة الخاصة للأفراد

المقصود بالحياة الخاصة في البحث هو كل ما يقوم به الشخص ولا يرضى أن يطلع عليه الغير[3]. فعدم توفر الحماية التقنية الفاعلة لما يتم تداوله من معلومات وأسرار ومراسلات عن طريق الانترنت، جعل الجرائم تمتد لتشمل الاعتداء على الحياة الخاصة كالتجسس أو تسجيل ونقل المحادثات والمراسلات الخاصة للأشخاص دون رضاهم، أو التقاط ونقل الصور الخاصة دون إذن أصحابها.

وقد عرف التعدي على الحياة الخاصة في الفضاء الإلكتروني صورا عديدة من بينها؛ التعدي على أسرار الآخرين بالاستعانة ببرامج خاصة يتنصتون بواسطتها على المحادثات التي تتم عن طريق الانترنت ويتم تسجيلها ثم نشرها على الشبكة العالمية بدون إذن أصحابها وذلك بغرض إلحاق الضرر بهم.

وما يعرف على برامج التنصت أنها تعمل على فتح منافذ في أجهزة المعتدى عليهم لتمكين المجرمين من الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الضحايا، ويتم تثبيت هذه البرامج خفية على أجهزة الضحايا وذلك عن طريق رسائل البريد الإلكتروني أو المواقع المغرية التي يزورها الضحايا، كأن يقوموا بالتنزيل المجاني لبعض البرامج التي يبحثون عنها وهم لا يعلمون بأنها مرفقة ببرامج خبيثة من شأنها التنصت على حياتهم الخاصة أو التقاط صورهم عن طريق التشغيل التلقائي لكاميرات الحواسيب دون علم أصحابها، كما يصعب في كثير من الأحوال الوصول إلى المعتدين لأنهم في الغالب يتسترون بأسماء مستعارة أو يستعملون الانترنت عبر فضاءات عمومية، أو يكونون في بلدان مغايرة وبالتالي يصعب التوصل إليهم وتحديد مواقع اتصالهم[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثاني: صور الجرائم الإلكترونية المتعلقة بالآداب العامة

بالرغم من الجوانب الإيجابية التي تقدمها الانترنيت إلا أنها كأي منتج بشري لها بعض الآثار السلبية والتي قد يكون من أكثرها خطورة على العقائد والأخلاق هو انتشار الجرائم الأخلاقية، كنشر وتوزيع المواد الإباحية وإتاحتها بين أيدي عامة المستخدمين، ولقد شكلت هذه الظاهرة تيارا جارفا يزحف على المجتمعات وعلى رأسها المجتمع الإسلامي مستهدفة في ذلك الانحلال العقدي والخلقي والقضاء على الهوية خاصة وأن غزو العقيدة والأخلاق أخطر من الغزو العسكري لأنه يؤدي إلى اعتلال الفكر والأخلاق لدى الأمم فتذهب شخصيتها وتزول معاني القوة فيها[1].

الفرع الأول: مفهوم الإباحية.

لقد لقي مفهوم الإباحية صعوبة كبيرة في تحديد تعريفا وضعيا شاملا لها ويرجع السبب في ذلك إلى صعوبة تحديد معنى الفحش الذي تشمله الإباحية بالنظر إلى اختلاف الثقافات والإيديولوجيات والأعراف، فقد يصنف عملا ما على أنه مادة إباحية بينما يصنف عند آخرين بأنه عمل خال من أي معنا جنسيا، وما يستخلص من التعريفات الواردة بشأن الإباحية أن كل مجموعة منها تتفق فيما بينها وفق أبعاد ثلاثة في مفهومها وذلك كما يلي:[2]

أولا ـــ البعد الوظيفي: يعرّف الإباحية بأنها كل ما يستخدم لغرض الإثارة الجنسية، وهو تعريف يربط علاقة المواد الإباحية بمدى درجة إثارتها للمستخدمين ومدى استجابتهم لها.

ثانيا ـــ البعد التصنيفي: وهو كل تعريف للإباحية يصدر من وجهة نظر الناس الرافضين لمثل هذه التصرفات؛ بمعنى كل عمل يرونه فاحش أو داعر فهو من الإباحية. وهو تعريف يشمل كل ما يعتقد الناس بأنه مادة تثير الأفكار الشهوانية كالابتذال الجنسي والعيب والاعتداء الجنسي.

ثالثا ـــ البعد النوعي: يعرّف المواد الإباحية بأنها كل ما ينتج بغرض إثارة الشهوة الجنسية لدى مستخدميها. وهو تعريف يربط الإباحية من وجهة نظر المؤلفين أو صناع المواد الإباحية الموجهة لجمهور المشاهدين والمستمعين والقراء بهدف إثارة رغباتهم الجنسية إلى أقصى حد ممكـــن من أجـــل

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

الحصول على أكبر قدر من الربح.

الفرع الثاني: أساليب الجرائم الإباحية ودوافعها

في الغالب يكون الربح المادي هو ما تسعى إليه المواقع الإباحية، حيث يستوجب على متصفح هذه المواقع دفع مبلغ معين مقابل مشاهدته لعرض إباحي، أو دفع اشتراك شهري أو سنوي مقابل الاستفادة من خدمات هذه المواقع التي تستدرج زبائنها يوميا عن طريق إرسال صور وإعلانات جنسية مجانية على عناوينهم البريدية.[1]

أما القوائم البريدية فغالبا ما تكون مجانية حيث يقوم أعضائها من المشتركين بتبادل الصور والأفلام الخليعة على عناوينهم الإلكترونية مما يشكل صعوبة المتابعة الأمنية لها، وحتى لو تم الانتباه إلى هذه القوائم لاحقا وتم حجبها فإن الحجب يكون قاصرا على المشتركين الجدد الذين لا يستعملون وسائل تجاوز المرشحات، أما الأعضاء السابقين فيصل إلى بريدهم الإلكتروني ما يريدونه دون تدخل وسائل الحجب، ويشترك في القوائم البريدية مئات الآلاف من الأشخاص حيث تصل كل رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعني تداول كم هائل من الرسائل والصور الجنسية كل يوم[2].

كما تعمل المواقع الإباحية بطرق شتى لاستقطاب أكبر عدد ممكن من المتصفحين دون مراعاة لعامل السن أو الدين، وذلك عن طريق نشر الرسائل البريدية العشوائية التي تقتحم خصوصيات المتصفحين والتي لا تعترف بأي حدود دولية أو جغرافية.

الفرع الثالث: أبعاد ظاهرة الإباحية على الانترنت

أظهرت دراسات إحصائية حديثة بأن حجم المواقع الإباحية بلغ 4.2 مليون موقع وهو ما يعادل 12 بالمائة من مجموع مواقع الانترنت، كما بلغ العدد اليومي لمتصفحي المواقع الإباحية عالميا 68 مليون متصفح وهو ما يعادل 25 بالمائة من متصفحي الانترنت في اليوم، وبلغت نسبة مستخدمي الانترنت الذين يتعرضون للإعلانات الإباحية بدون إرادتهم 34 بالمائة، كما بلغ مجموع المواد الإباحية التي يتم تحميلها شهريا إلى الحواسيب الخاصة 1.5 مليار وهو ما يعادل 35 بالمائة من مجموع التنزيلات شهريا،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما بلغت النسبة الإجمالية لمرتادي المواقع الإباحية 42.7 بالمائة من مجموع مستخدمي الانترنت، وقدر مجموع متصفحي المواقع الإباحية الخاصة بالبالغين 72 مليون متصفح شهريا على مستوى العالم.[1]

ورغم أن نسبة 12 بالمائة من مجموع مواقع الانترنت تعد رقما ضئيلا نسبيا إلا أن خطورة المواقع الإباحية وما تلحقه بالأفراد والمجتمعات من أضرار كفيلة بتحديد ضخامة المشكلة، خاصة وأن هذه الظاهرة تستهدف جميع أفراد المجتمع دون مراعاة للسن أو الجنس، حيث بلغ مجموع الطلب اليومي على مواقع الأطفال الإباحية 116000 طلب، كما بلغ عدد المواقع الإباحية التي تروج دعارة الأطفال 100000 موقع (علما بأن الموقع الواحد يحتوي على مئات الصفحات التي تعرض الآلاف من الصور)[2].

الفرع الرابع: الآثار الاجتماعية للمواد الإباحية

لقد أثبتت الدراسات العلمية المكثفة مدى تأثير المشاهدة على السلوك والتفكير، وقد صرح في ذلك الدكتور الأمريكي براندون المتخصص في دراسة مصادر الأمراض (Epidemiology) أنه لو لم يخترع جهاز التلفاز لشهدت أمريكا في هذا العصر انخفاض في الإجرام بنسبة عشرة آلاف جريمة قتل سنويا، وسبعين ألف جريمة اغتصاب، وسبعمائة ألف جريمة عنيفة، وقد توصل الدكتور براندون إلى هذه النتائج إثر دراسة دامت أقرب من ثلاثين سنة[3]، وهي دراسة واحدة من ضمن عدد كبير جدا من الدراسات المشابهة التي تثبت مدى تأثر البشر بما يشاهدونه والتأثير السلبي لتلك الوسائل على سلوكهم.

كما لاحظ عالم النفس الدكتور ادوارد دونرستين من جامعة وسكونسون بأمريكا بأن الذين يخوضون في الدعارة والإباحية غالبا ما يؤثر ذلك في سلوكهم من زيادة في العنف وعدم الاكتراث لمصائب الآخرين وتقبل لجرائم الاغتصاب[4].

وفي تحقيقات الاستخبارات الأمريكية (FBI) حول جرائم الاغتصاب، اكتشفوا أن 80% من الحالات يتم العثور فيها على مواد إباحية إما في موطن الجريمة أو في منزل الجاني[5]، كما تفيد دراسة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة

...../...

أجراها الدكتور وليام مارشال اعترف فيها 86% من المغتصبين بأنهم يداومون على استخدام المواد الإباحية، واعترف 57% منهم بأنهم كانوا يقلدون أحد المشاهد التي تأثروا بها من المصادر الإباحية حين تنفيذهم لجرائهم [1].

كما أجريت دراسة لـــ 1400 حالة من جرائم اغتصاب الأطفال حصلت في مدينة لويسفيل الأمريكية ما بين السنوات 1980 و1984م، حيث ضُبط بحوزة جميع المجرمين مواد إباحية للبالغين، كما ضبط عند أغلبهم صورا خليعة للأطفال[2]، ونظرا لضخامة المأساة بحث مجلس النواب الأمريكي في هذا النوع من الجرائم وتوصلوا إلى أن أكثر سمة موحدة بين هؤلاء المجرمين هو تداولهم للصور المحرضة على اغتصاب الأطفال[3].

ويقول الدكتور فيكتور كلاين بعد دراسته لمجموعة كبيرة من مدمني المواد الإباحية، أن عدم حجب هذه المواد يشكل إغراء شديدا على الأفراد قد يصل إلى حد الإدمان فيصبحون عبادا للشهوات حتى لو كلف ذلك فقدانهم لأموال ضخمة، كما حذر مما تبثه القنوات الفضائية من إباحية في المنازل والذي كان من نتائجها زنا المحارم سواء لدى البالغين أو المراهقين والأطفال، وقد بيّن الدكتور فيكتور في دراسته أن الكثير من المعتدين لا يُعرف عنهم سوء الخلق أو فعل الشر كالرجل المتفوق في دراسته، والرئيس لشركته والفاعل للخير الذي ظهر بعد ذلك أنه كان يغتصب النساء بحد السكين أو المسدس في منطقتي فينكس وتوسون الأمريكية، وكان الدافع الوحيد لهذه الأعمال هو تشبع المجرم بالمواد الإباحية منذ فترة طويلة[4].

كما يجر التعرض للوسائل الإباحية إلى تبعات وعواقب أسرية واجتماعية لا تحمد عقباها، حيث تفيد الإحصاءات أن 33% من ضحايا الاغتصاب يفكرون بالانتحار أو ينتحرون[5]، كما أن 80% من ضحايا الاعتداء الجنسي من الأولاد الذكور يصبحون بعد ذلك مدمنين لأنواع المخدرات

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والمسكرات، و50% منهم يفكر بالانتحار، و23% منهم يقدم على الانتحار، و70% تبقى معهم عقد نفسية[1].

وإن طرحي لهذه الأمثلة من الجرائم التي كلها مستوحاة من العالم الغربي لا يعني تعفف العالم العربي بصفة عامة والعالم الإسلامي على الخصوص من مثل هذه الجرائم، وإنما من وجهة نظري فإن الدراسات المتخصصة في هذا الجانب أجدها أكثر تحليلا وواقعية في البحوث الغربية منها في البحوث العربية والإسلامية التي كثيرا ما تعتمد المنهج النظري وتفتقر كثيرا إلى التعمق في أسباب الظاهرة مقارنة بالواقع.

كما أوافق البحوث والدراسات التي تجعل من ارتياد المواد الإباحية أحد الأسباب الرئيسية لارتكاب الجرائم الجنسية بشتى أنواعها، وخاصة زنا المحارم والتعدي الجنسي على الأطفال، فما لاحظته قبل انتشار القنوات الفضائية والانترنت إلى نهاية الثمانينات كانت جرائم الزنا في بلدنا على سبيل المثال تكاد تعد على الأصابع وأغلبها يقع بين البالغين من الجنسين وسرعان ما يفضح أمرهم ويلقون العقاب القانوني، لكن بعد ظهور القنوات الفضائية تفشت ظواهر غريبة من الجرائم الجنسية كظاهرة اغتصاب النساء واختطافهن والتحرش بهن علنا، وقد ازداد الأمر ضراوة بعد اكتساح الانترنت المحلات التجارية والبيوت حيث برزت ظاهرة اختطاف الأطفال من الجنسين والتعدي عليهم جنسيا ثم يقتلون في معظم الأحيان، كما برزت ظاهرة التخنث والشذوذ الجنسي العلني، ناهيك عن التصرفات المشينة الصادرة من بعض الشباب خاصة المثقف منهم؛ كظاهرة التبرج الفاضح والمغازلة العلنية وغيرها من الصور التي لا تمت لعقيدتنا وأعرافنا بصلة، كما أكاد أجزم بأن السبب الأساسي في تفشي هذه الظواهر بعد ضعف الوازع الديني هو سوء استخدام التقنية الحديثة كالتعرض للمواد الإباحية وأنواع الجرائم.

ولقد بدت آثار الإباحية ظاهرة للعيان، حيث صرح الأمن الوطني في سنة 2007 بأرقام مخيفة سجلتها مصالحه عن حالات العنف التي تعرض لها الأطفال خلال هذه السنة والتي بلغت 4875 حالة، تعرض خلالها 1546 طفل لاعتداءات جنسية، وقتل 25 منهم، أما عن جريمة الاختطاف التي بدأت

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة

...../.....

تتنامى خلال هذه السنة فقد سجلت الجزائر146 حالة[1]، وفي مداخلة ألقاها كل من الدكتور عبد الرزاق فروي والدكتور بن إسماعيل من كلية الطب بجامعة قسنطينة[2]، كشفا فيها بعض الأرقام التي سجلتها مصالح الطب الشرعي عبر الوطن خلال سنة 2011، حيث تعرض 5000 طفل للعنف من بينهم 33 بالمائة تعرضوا إلى اعتداءات جنسية، كما سجلت ولاية قسنطينة لوحدها 244 حالة عنف ضد الأطفال خلال نفس السنة من بينها 19 بالمائة اعتداءات جنسية، وحسب الدكتور عبد الرزاق فروي فإن نسبة الأطفال الأكثر عرضة للاعتداءات الجنسية هي الشريحة العمرية بين 6 و 10 سنوات مؤكدا بأن نتائج العنف على الأطفال تكون في الغالب وخيمة، حيث تنعكس مباشرة على الطفل وصحته من خلال انحراف سلوكه الذي يتجه أحيانا للإدمان على التدخين والمخدرات أو الانهيار العصبي وأحيانا يصل الأمر إلى الانتحار.

وفي سنة 2012، كشف البحث الذي قدمه المدير الولائي للشرطة القضائية بولاية المدية الجزائرية خلال اليوم الدراسي المنظم من قبل ديوان مؤسسات الشباب بالمدية حول العنف ضد الأطفال، عن تسجيل المصالح الأمنية على المستوى الوطني لـــ 1737 اعتداء جنسي مورس ضد الأطفال خلال هذه السنة[3]، ولقد بينت التحقيقات التي قامت بها مصالح الأمن أن تفشي هذه الظاهرة له علاقة بمجموعة من الأسباب، من بينها التعرض للمواد الإباحية والجرائم المتاحة على الانترنت والفضائيات نظرا لخطورتها في تغذية السلوك الإجرامي تجاه شرائح معينة من المجتمع كالأطفال والنساء، خاصة وأن التكنولوجيا الحديثة وما حوته من سلبيات ظهرت واستفحلت بالوطن خلال السنوات الأخيرة وبقيت دون رقابة أسرية أو حكومية بينما ضراوة المواقع الإباحية وموادها تزداد كل يوم.

الفرع الخامس: مداخيل الصناعة الإباحية

يعتبر تحقيق الربح المالي من الأهداف الأساسية في الصناعة الإباحية، وهو ما تؤكده الدراسة التي نشرتها وزارة العدل الأمريكية[4]، حيث ذكرت أن تجارة الدعارة والإباحية هي تجارة رائجة ولها

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

أواصر وثيقة تربطها بالجريمة المنظمة، كما تفيد إحصاءات الاستخبارات الأمريكية (FBI) بأن تجارة الدعارة هي ثالث أكبر مصدر دخل للجريمة المنظمة بعد المخدرات والقمار حيث بلغت 85% من أرباح المواد الإباحية المنشورة ورقيا أو على الانترنت[1].

وعلى المستوى العالمي بلغت صناعة المواد الإباحية في سنة 2004م حوالي 57 بليون دولار أمريكي، وهو رقم يوازي الميزانية السنوية لعشرات الدول النامية، كما بلغت صناعة المواد الإباحية على الانترنت في نفس السنة حوالي 2.5 بليون دولار أمريكي من مجمل الصناعة عالميا أي 4 بالمائة من مجمل صناعة المواد الإباحية بشكل عام، وهي نسبة لا تفسر قلة انتشار هذه المواد على الانترنت بل تعني تدني تكلفة نشرها على المواقع الإباحية.

والجدول التالي يظهر مداخيل صناعة المواد الإباحية خلال سنة 2004 [2].

جدول رقم: (03) يبين مداخيل صناعة المواد الإباحية خلال سنة 2004

نوع المواد الإباحية	حجم مداخيل صناعتها
أفلام الفيديو الجنسية	20 بليون دولار أمريكي
المجلات الجنسية	7.5 بليون دولار أمريكي
تلفون الجنس	4.5 بليون دولار أمريكي
المواد الإباحية في الانترنت	2.5 بليون دولار أمريكي
خدمات المرافقة	11 بليون دولار أمريكي
نوادي الجنس	5 بليون دولار أمريكي
المواد الإباحية في الأقراص المضغوطة	1.5 بليون دولار أمريكي
الأدوات الجنسية	1 بليون دولار أمريكي
أخرى	1.5 بليون دولار أمريكي

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

ولقد بلغ عدد زائري المواد الإباحية على الانترنت سنة 2004م حوالي 73 مليون زائر، ورغم أن الكثير من القوانين الدولية تمنع دعارة الأطفال وعرض المواد الإباحية عنهم إلا أنه رصد حوالي 100 ألف موقع يعرض مواد إباحية لهذه الفئة تستجيب لطلبات الشواذ من زبائن دعارة الأطفال[1].

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

الفصل الثالث:
الجرائم الإلكترونية المتعلقة بأمن الدول والمجتمعات

المبحث الأول: جرائم التجسس الإلكتروني

المبحث الثاني: الجريمة المنظمة عبر الانترنت

المبحث الثالث: الإرهاب الإلكتروني

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: جرائم التجسس الإلكتروني

لقد أصبحت المعلومات من المعايير الأساسية التي يقاس بها قوة الشعوب، فمن يملك المعلومات وله القدرة على حمايتها يمكنه أن يسيطر، ولذلك كان من الطبيعي أن تكتسب أهمية المعلومات بعدا عسكريا وسياسيا وأصبحت السلاح الجديد الذي تحارب به الدول المتحكمة في المعلوماتية، كما أصبح الحاسوب أداة هامة من أدوات الحرب الاقتصادية والإعلامية وحرب السيطرة خاصة بعد تغلغله في كل الميادين، فمن يعلم سوف ينتصر حتى لو لم يكن هو الأقوى ومن لا يعلم سوف ينهزم[1] ، وكان من نتاج ذلك ظهور جرائم جديدة غير متوقعة من جرائم نظم المعلومات طالت أمن الدول والمجتمعات وعلى رأسها التجسس الإلكتروني.

المطلب الأول: مفهوم التجسس وأنواعه

الفرع الأول: مفهوم التجسس.

أولا ـــ التعريف اللغوي للتجسس:

التجسس في اللغة هو اللمس باليد، وجسّ الخبر: أي بحث عنه، وتجسس الأمر: أي تفحصه وتطلبه وبحث عنه، وقيل التجسس بالجيم: هو التفتيش عن بواطن الأمور وأكثر ما يقال في الشر والجاسوس صاحب سر الشر[2].

ثانيا ـــ التجسس في الاصطلاح الفقهي:

لم يفرد الفقهاء مصطلح التجسس ببحث مستقل وإنما ذكر مع مواضيع ذات صلة، حيث ورد التجسس صراحة في القرآن الكريم في قوله تعالى: ﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجْتَنِبُواْ كَثِيرًا مِّنَ ٱلظَّنِّ إِنَّ بَعْضَ ٱلظَّنِّ إِثْمٌ وَ لَا تَجَسَّسُواْ وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَٱتَّقُواْ ٱللَّهَ إِنَّ ٱللَّهَ تَوَّابٌ رَّحِيمٌ ﴾[3] والمراد من الآية، النهي عن تتبع عورات المسلمين وعيوبهم، واستكشاف ما ستر الله تعالى، كما قرئ بالحاء المهملة (ولا تحسسوا) من الحـــس الذي هو أثر الجس وغايته، والمراد

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

بالقراءتين: النهي عن تتبع العورات مطلقا، واعتباره من الكبائر[1].

وجاء في تفسير القرطبي، أن التجسس بالجيم؛ هو البحث عما يكتم عنك[2].

ثالثا ــ مفهوم التجسس في القانون الوضعي:

عرف التجسس في القانون الوضعي تعريفات عديدة لم يسلم معظمها من النقد، و يرجع ذلك إلى صعوبة الوصول إلى تعريف دقيق ومنضبط للتجسس بسبب تطوره وتشعبه ولكونه يمس جوانب متغيرة ومتجددة سواء كانت هذه الجوانب سياسية أم عسكرية أو اقتصادية، وقد تكون أيضا اجتماعية أو معنوية أحيانا[3]. ومن بين التعريفات القانونية للتجسس؛ هو البحث والتنقيب عما يتعلق بالعدو من معلومات باستخدام الوسائل السرية والفنية، ونقل هذه المعلومات بذات الوسائل أو عن طريق العملاء والجواسيس بغرض الاستفادة منها في إعداد الخطط، كما يعرّف القانون الدولي العام الجاسوس بأنه: "الشخص الذي يعمل في خفية، أو تحت ستار مظهر كاذب، في جمع ــ أو محاولة جمع ــ معلومات عن منطقة الأعمال الحربية لإحدى الدول المتحاربة، بقصد إيصال تلك المعلومات لدولة العدو"، ولقد نصت المادة "التاسعة عشرة" من لائحة "لاهاي" للحرب، على الآتي: يُعدُّ جاسوسا، ذلك الذي يعمل سرا، أو من وراء ستار زائف، للحصول على معلومات في منطقة العمليات، بنية تبليغها للفريق الخصم[4].

الفرع الثاني: أنواع التجسس

في وقتنا الحاضر أصبح التجسس نوعين؛ التجسس التقليدي، والتجسس الإلكتروني.

أولا ــ التجسس التقليدي: يعتمد التجسس التقليدي كليا على ما يقوم به الجاسوس نفسه من جمع للمعلومات سواء كان بالعين المجردة أو باستخدام الحواس الخمس كلها، ويكون ذلك سرا أو بادعاء وهمي للاستيلاء على معلومات سرية بقصد إبلاغها إلى جهة معادية[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثانيا ــ التجسس الإلكتروني: يعتمد التجسس الإلكتروني على استخدام التقنية الحديثة في الحصول على المعلومات، ومن أهم أنواعه ما يلي:

1 ــ التجسس عن طريق الانترنت[1]:

عرف هذا النوع من التجسس انتشارا واسعا خاصة بين مستخدمي الكمبيوتر الشخصي بشكل عام، حيث يعتمد فيه على برامج خارجية مبنية على أساس ما يعرف بالعميل والخادم Client وServer ويشترط لتفعيل عملية التجسس الإلكتروني أن يعمل برنامج الخادم في النظام المستهدف. ولقد عرفت الحواسيب برامج تجسسية عديدة لأنظمة ويندوز windows و لينكس Unix من أشهرها: Sub7, Netbus, Backorifice ، كما لم تسلم أيضا الأجهزة المحمولة من برامج التجسس التي تعمل بنفس الطريقة المذكورة ومن أمثلتها برنامج التجسس FlexiSPY ، وهو برنامج يثبّت على الهواتف النقالة للتجسس على المكالمات والرسائل القصيرة SMS وسجل المكالمات وغيرها. وما ساهم في ذلك أن بناء برامج التجسس هو في غاية البساطة نظرا لإمكانية استخدام لغات البرمجة المعروفة عالميا كلغة البرمجة: السي C ، والسي++ (C++)، والباسكال Paskal ، والفيجول بيسيك Visual Basic ، حيث تتم برمجة الخادم وفق ثلاث نقاط أساسية:

1 ــ فتح منفذ port في الجهاز المستهدف.

2 ــ استقبال الأوامر من خلال المنفذ.

3 ــ تنفيذ الأوامر التي تأتي من المنفذ.

ثم يلي ذلك دور البرنامج العميل في الطرف الآخر ويتم برمجته على أساس:

1 ــ إجراء اتصال مع الخادم من خلال المنفذ في الطرف الآخر.

2 ــ إرسال الأوامر للخادم من خلال المنفذ المحدد.

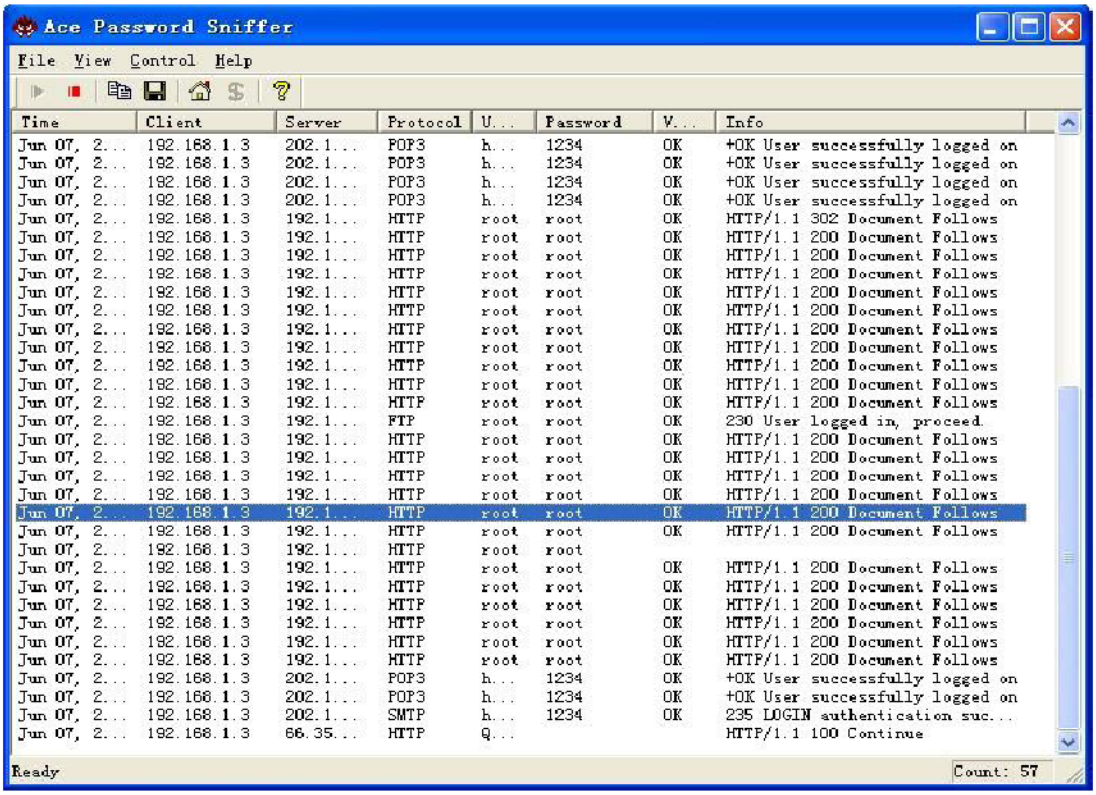
3 ــ استقبال المعلومات والنتائج.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...



الشكل(17): يبين أحد برامج التجسس المستعملة في الانترنت للحصول على كلمات المرور الخاصة بالبريد الإلكتروني[1]

2 ــ التجسس من خلال الشبكات السلكية واللاسلكية[2] :

وهو أحد صور التجسس الالكتروني على الشركات والهيئات التي تستخدم الشبكات بكل أنواعها الصغيرة والكبيرة السلكية واللاسلكية، حيث يتم اصطياد حزم البيانات المرسلة بما يعرف بـــطريقة Sniffer ، ويستعين الجواسيس في ذلك على برامج تعمل تحت أنظمة الويندوز ولينكس كبرنامج Ethereal الموجه للتجسس على الشبكات الداخلية، وبرنامج Tcpdump و Widnump وغيرها من البرامج التي تعمل على اصطياد البيانات المرسلة داخل الشبكة، كما تعمل على مراقبة أغلب البروتوكولات مما يتيح للجاسوس الذي يستخدم شبكة محلية من الوصول والتجسس على بقية المستخدمين كالحصول على كلمات المرور السرية للبريد الإلكتروني، ولقد ظهر برنامجا تجسسيا أكثر خطورة من سابقيه يعرف بـــ Cain & Abel Pasword Recovery وهو برنامج يتحدى بروتوكولات التشفير التي تصد الاختراق، حيث يمكنه التجسس على كل أنواع البروتوكولات وباستطاعته فك تشفير كلمات المرور، كما تم برمجة نسخة منه للتجسس على الأجهزة المحمولة أيضا.

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../.....

وفيما يخص الشبكات اللاسلكية فقد تم تعديل خاص مع إضافات جديدة على برامج التجسس المذكورة وهي طريقة تعرف بـــ Wireless Sniffer لأن البيانات المرسلة عبر الشبكات اللاسلكية تحتوي على مفتاح تحقق يكون مشفرا لحماية البيانات أثناء الإرسال ومن أشهر أنواع مفاتيح الحماية WEP و WPA لكن تم كسر تشفيرهما لمفاتيح الحماية، ومن أشهر برامج التجسس في هذا المجال برنامج Kismet لأنظمة لينكس وبرنامج NetStumbler الذي يعمل على أنظمة الويندوز حيث يتم من خلالهما تحديد البيانات والأجهزة المتصلة، ومن خلالهما يتم التقاط البيانات أو تزييفها أو كسر مفتاح التشفير وذلك اعتمادا على حزمة مساعدة من البرامج مثل:

ـــ Airdump وهو يستعمل في اصطياد حزم البيانات المرسلة بين الأجهزة.

ـــ Aireplay ويستعمل لإعادة حقن بيانات في الحزم المرسلة من أجل تزييف البيانات الأصلية.

ـــ Aircrack يستعمل لكسر تشفير مفتاح التحقق في الشبكات اللاسلكية.

3 ـــ التجسس الإلكتروني على الهاتف المحمول[1]:

في سنة 1989م ظهر نوع من التشفير اسمه GSM A5 استخدم في الهواتف النقالة والانترنت اللاسلكي WIFI وبرامج تحديد المواقع GPS وغيرها، وهو برنامج يعمل على حماية وتشفير البيانات المرسلة بين الأجهزة المحمولة ومحطة الاستقبال من محادثات صوتية أو رسائل قصيرة أو فاكس وغيرها، ثم ظهر نوعان من هذا التشفير GSM A5.1 و GSM A5.2 فيستخدم النوع الأول في أوروبا وأمريكا وهو الأقوى في التشفير عالميا، بينما يستخدم النوع الثاني GSM A5.2 في الدول الأخرى وهو ضعيف مقارنة بالأول رغم أن عدد الذين استخدموه في سنة 2000 بلغ 130 مليون مستخدم، ولقد عرف هذا النوع من التشفير انتشارا كبيرا في شبكات GSM والثريا لما عرف عنه من تصديه للهجمات التجسسية. ورغم ذلك تم كسر هذا النوع من التشفير بواسطة برنامج بالغ الخطورة تم تطويره خصيصا لهذا المجال المعروف ببرنامج: CrytoPro GSM A5 الذي اكتشف سنة 2006م وهو يلتقط المحادثات والرسائل القصيرة بدقة عالية مما اضطر بالمنتجين إلى إضافة تعديلات علىGSM ليكون أكثر حماية في وجه برامج التجسس.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

4 ــ التجسس الإلكتروني على الموجات والترددات[1]:

لا تعد أغلب الموجات والترددات سرية ومن بينها موجات محطات الراديو ــ الإذاعة المسموعةــ التي تسمع على موجات محددة مثل FM حيث يمكن استقبالها عن طريق جهاز المذياع أو الهاتف المحمول، أو التلفاز، أو جهاز الكمبيوتر، وتوزع الترددات والموجات اللاسلكية كما يلي:

ــ مجال موجات الراديو البعيدة من KHz30 إلى KHz300 وهي موجات تستخدمها محطات الراديو.

ــ مجال موجات الراديو القريبة من MHz3 إلى MHz30 وتستخدمها محطات الراديو المعروفة أيضا.

ــ مجال موجات الراديو العالية وهي التي تستخدم في اللاسلكي للأسلاك الأمنية من MHz30 إلى MHz300.

ــ مجال الموجات الهوائية وتستخدم غالبا في الطائرات ومحطات التلفزيون من MHz300 إلىGHz3.

ــ مجال الموجات الدقيقة وتستخدم في الأقمار الصناعية والرادار ومحطات التلفزيون أيضا من GHz3 إلى GHz30.

ويستعمل الجواسيس عدة طرق للتجسس على الترددات الدولية معتمدين في ذلك على خبرتهم في البرمجة بشكل عام والتشفير بشكل خاص للحصول على الترددات المستهدفة باستعمال التقنية الحديثة، كما يعتمدون أيضا على البحث المكثف عبر الموجات أو الوصول إليها بالصدفة، وبذلك يتم التجسس على البيانات أو حقنها وتغييرها في الترددات والموجات باستخدام برامج معلوماتية كبرنامج Aireplay حيث يتم حقن بيانات في الترددات اللاسلكية الدقيقة جدا كتغيير بث قناة تلفزيونية في بلد ما أو إعطاء إحداثيات خطأ للطائرات التي تقصف في الحرب.

5 ــ التجسس الإلكتروني من خلال الأقمار الصناعية:

وهو من أنواع التجسس الدولي الذي تستخدم فيه أجهزة سرية و جدّ معقدة لا يمكن للباحث الوصول إليها، لكن ما يمكن استنتاجه هو أن التجسس عن طريق الأقمار الصناعية لا يمكن أن يقوم به فرد أو منظمة وإنما يقتصر على الدول المتقدمة التي تسيطر على كل البيانات في العالم وتملك أقمارا صناعية.[2]

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثاني: صور التجسس الإلكتروني وآثاره:

لقد رصدت العديد من حالات التجسس الإلكتروني الدولي وعلى رأسها ما اكتشف مؤخرا عن مفتاح وكالة الأمن القومي الأمريكية (NSA) التي قامت بزراعته في نظام التشغيل الشهير ويندوز Wnidows الأمر الذي أدى إلى الاعتماد على أنظمة بديلة عند بعض الدول المتطورة كألمانيا مثلا، كما كشف النقاب عن شبكة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كندا، وبريطانيا، واستراليا ونيوزيلندا ويطلق عليها اسم (ECHELON) وهي مختصة في رصد المكالمات الهاتفية والرسائل بأنواعها سواء ما كان برقيا، أو عن طريق التلكس أو الفاكس أو البريد الإلكتروني أو رسائل الهواتف الذكية SMS ، ولقد خصص هذا النظام للتعامل مع الأهداف غير العسكرية حيث يعترض كميات هائلة من الاتصالات والرسائل الإلكترونية عشوائيا باستخدام خاصية الكلمة المفتاحية بواسطة الحواسيب المتعددة الموزعة على العديد من المحطات السرية حول العالم لمراقبة شبكات الاتصالات الدولية التي تلتقط المعلومات عن طريق الأقمار الصناعية والشبكات الخاصة بالاتصالات الدولية كما ترصد أيضا الاتصالات الأرضية وكذا الشبكات الإلكترونية، وبذلك فإن الأفراد والحكومات الذين لا يستخدمون أنظمة التشفير لحماية شبكاتهم وأجهزتهم سيكونون أهدافا سهلة لشبكة التجسس هذه، وإن كان هذا لا يعني بالضرورة أن الأهداف الأخرى التي تستخدم أنظمة التشفير في مأمن تام من الغزو التجسسي خاصة إن كانت أنظمة التشفير مستوردة، كما لم يقتصر التجسس الحديث على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات الصناعية والاقتصادية والاجتماعية..[1]

ونظراً لكون التجسس الاقتصادي يستهدف في المقام الأول شركات تجارية فإن خدمات التجسس والتجسس المضاد أصبحت سلعة رائجة، ولما كانت الولايات المتحدة أول مكان تتبلور فيه الظاهرة فقد أصبحت أول مكان تظهر فيه وكالات تجسس خاصة تقدم خدماتها للشركات تحت اسم "الاستخبارات التنافسية" ويقصد بها "جمع المعلومات الصناعية وتحليلها وتوزيعها".

وعلى الرغم من الفوائـــد التي تعود على الشركات العالمية جراء التجسس الاقتصادي، إلاّ أن

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

خسائره طالت العديد من الشركات الأخرى إذ أكد مجموعة من الخبراء في ألمانيا أن عمليات التجسس الاقتصادي والصناعي ضد الشركات الألمانية تهدر نحو (50) ألف فرصة عمل سنوياً، ونقلت وكالة الأنباء الألمانية عن أحد الخبراء الأمنيين عجز الكثير من شركات البلاد عن مواجهة عمليات التجسس على مشاريعها وتصميماتها من قبل الشركات الأجنبية، بالإضافة إلى ضعفها في مواجهة قراصنة الكمبيوتر، كما أن خسارة الشركات الألمانية للمعرفة والخبرة الفنية بسبب عمليات التجسس أدى إلى فقدان القدرة على المنافسة وإهدار فرص العمل داخل البلاد، كما أن حجم الخسارة التي يتعرض لها الاقتصاد الألماني سنوياً من عمليات التجسس تتراوح بين (10 إلى 50) مليار يورو.

وفي الولايات المتحدة الأمريكية قُدّرت الخسائر الناتجة عن التجسس المحلي والأجنبي على الشركات الأمريكية فيما يتعلق بخسائر حقوق الملكية الفكرية بحوالي (300) بليون دولار أمريكي في العام 1997م، وعلى الرغم من وجود قانون التجسس الاقتصادي في الولايات المتحدة الذي اعتمد سنة 1996م، إلاّ أن العديد من الدول الأجنبية قد استهدفت الشركات الأمريكية بشكل خاص بعمليات تجسس منظمة في سبيل اختراقها والحصول على آخر ما توصلت إليه من تكنولوجيا، حيث تنفق الولايات المتحدة أكثر من 108 بلايين دولار على الأبحاث والتطوير وهو ما يعادل ربع الإنفاق العالمي كله. وعلى الرغم من العقوبات الشديدة التي فرضها قانون التجسس الاقتصادي والمتضمنة غرامات تصل إلى عشرة ملايين دولار والسجن لمدة 15 سنة إلاّ أن قضايا التجسس تعرف تزايد مستمر.[1]

ومن الصور الحديثة للتجسس الإلكتروني على سبيل المثال الخبر الذي جاءت به جريدة سكاي نيوز الإلكترونية[2] حول وثائق نشرتها صحيفة الغارديان البريطانية، مفاده أن الاستخبارات الأميركية تستخدم برنامجا سريا لمراقبة الانترنت يدعى "إكس كيسكور" يتيح لها أن تراقب "كل ما يقوم به المستخدم على الإنترنت."

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

وأكدت الصحيفة البريطانية نقلا عن وثائق جديدة سربها الأميركي إدوارد سنودن المطلوب للولايات المتحدة، أن برنامج "إكس كيسكور X-Keyscore " يتيح لوكالة الأمن القومي التي تستخدمه أكبر قدر من المراقبة عبر الإنترنت، حيث يتم عن طريقه المراقبة المباشرة لكل الرسائل الإلكترونية وعمليات البحث عبر الإنترنت أو أي استخدام لشبكات التواصل الاجتماعي أو أي عمل آخر يقوم به شخص ما على الإنترنت. ويعمل هذا البرنامج بالاعتماد على حوالي 700 خادم موزعة في أنحاء العالم بما في ذلك روسيا والصين وفترويلا.

ومن الأمثلة التي أوردها الغارديان في هذا الأمر عملية بحث يقوم بها شخص مستخدما لغة غير متداولة كثيرا في منطقته الجغرافية كالبحث باللغة الألمانية في باكستان، أو حتى عملية بحث يقوم بها شخص ما عبر موقع غوغل للخرائط لمكان يمكن أن يشكل هدفا لاعتداء إرهابي.

كما كشفت الصحيفة في مطلع جوان سنة 2013م، عن برنامج يدعى PRISM تستخدمه الاستخبارات الأميركية للدخول إلى أنظمة كبرى شركات الإنترنت لجلب أية معلومات تحتاجها عن أي مستخدم لتلك الشركات وبدون أية عقبات.

وبناء على ذلك فإن المجتمع المعلوماتي لا يستطيع ممارسة خصوصياته بحرية في الفضاء الإلكتروني كما لا يمكنه التأكد من أن أنشطته على الويب هي مصانة أم مراقبة من طرف المتربصين به، وهو ما يؤثر سلبا على موثوقية التعامل بالانترنت رغم كونها أحد الوسائل الأكثر حيوية في الحياة المعاصرة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني: الجريمة المنظمة عبر الانترنت

إلى جانب الأنشطة الإجرامية التقليدية التي عرفت بها المنظمات الإجرامية كالاتجار في المخدرات، وتهريب الأسلحة والمواد النووية، والاتجار في السيارات المسروقة، والتهرب الضريبي والجمركي، وتهريب العمالة غير الشرعية، وتجارة البشر، والتزييف والتزوير.. فإنها لم تتوان في استغلال التكنولوجيا الجديدة التي وجدت فيها مناخا ملائما لازدهار واتساع أنشطتها إضافة إلى تبييض عائداتها على المستوى الدولي، حيث قدر حجم الأموال المتحصلة من أنشطة المنظمات الإجرامية التي يتم غسلها سنويا بحوالي 500 مليار دولار وهو مبلغ يتجاوز الناتج القومي لعدة دول[1]، وبذلك استطاعت أن تجمع ثروات طائلة كان لها أثر كبير في زعزعة الأنظمة الاقتصادية والديمقراطيات الحديثة[2].

المطلب الأول: مفهوم الجريمة المنظمة.

لم يرس مفهوم موحد للجريمة المنظمة، ويرجع السبب في ذلك إلى ما تتسم به من غموض وعدم الوضوح، فهناك مفاهيم كثيرة تتعلق بالجريمة المنظمة تختفي عندها أنواع عديدة من الأفعال الإجرامية وأشكال مختلفة من المنظمات الإجرامية؛ فالمافيا، والجريمة المنظمة، والإجرام المنظم، والإجرام المحترف، والإجرام الاقتصادي لا تتضح معالمها في مفهوم الجريمة المنظمة وكثيرا ما تستخدم كمترادفات[3]، وبناء على ذلك صنفت الجريمة المنظمة وفق المفهوم الأمني لها، والمفهوم الإجرامي، والمفهوم القانوني.

الفرع الأول: المفهوم الأمني للجريمة المنظمة

لقد تم تسجيل مفاهيم عديدة في هذا الجانب اعتمدت كلها على العنصر الأمني البحت، وهي مفاهيم صادرة عن الهيئات الأمنية كالبوليس الدولي Interpol، ومكتب التحقيقات الفيدرالية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

الأمريكية FBI، حيث يعرّف الانتربول الجريمة المنظمة بأنها: "جماعة من الأشخاص تقوم بارتكاب أفعال غير مشروعة بصفة مستمرة، وتهدف إلى تحقيق الربح بصفة أساسية، دون التقيد بالحدود الوطنية"[1] ، كما عرفها أيضا بأنها: "جماعة من الأشخاص تتمتع بهيكل تنظيمي وتهدف إلى تحقيق الربح عن طريق ارتكاب أنشطة غير مشروعة، مستخدمة التخويف والرشوة"[2] ، والملاحظ على مجموع المفاهيم الأمنية أنها تركز على الجانب العملي للجريمة المنظمة ومدى خطورتها على الأمن العام[3]، وذلك من خلال وصفها بمجموعة من الدلائل أهمها:

1 ــ دلائل تتعلق بأساليب التخطيط والتحضير؛ كالتخطيط الدقيق والمنظم، والتوافق الجيد مع الأسواق المشروعة وغير المشروعة.

2 ــ دلائل تتعلق بتنفيذ الأفعال الإجرامية؛ كاستخدام أساليب المعرفة والتكنولوجيا الحديثة.

3 ــ دلائل تتعلق بأساليب استخدام متحصلات الجريمة؛ كالاتجاه إلى الربحية المرتفعة، اللجوء إلى غسل الأموال وإعادة ضخها في الاقتصاد المشروع.

4 ــ دلائل تتعلق بهيكل التنظيمات؛ كالتدرج وعلاقات السلطة والتبعية المعقدة.

5 ــ دلائل تتعلق بأساليب مساعدة أعضاء الجماعة؛ كالمساعدة على الهرب، تسخير المحامين والمستشارين القانونيين، تسديد الكفالات الضخمة، التهديد والترويع وخطف الشهود، والمساعدة أثناء الحجز وإعانات المعيشة المقدمة للأقارب.

6 ــ الدلائل المتعلقة بأساليب الضغط واستغلال النفوذ؛ كفرض التبعية عن طريق المخدرات والألعاب غير المشروعة قانونا، والجنس، والقروض، وشراء أصوات الناخبين، والرشوة.

7 ــ دلائل لها علاقة بالدعاية والعلاقات العامة؛ كالضغط والتأثير والسيطرة على وسائل الإعلام.[4]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني: مفهوم علم الإجرام للجريمة المنظمة

عرف هذا النوع أيضا العديد من التعريفات المقدمة من علماء الإجرام؛ حيث يرى الأستاذ CUSSON أن المقصود من الجريمة المنظمة أنها: "منظمة إجرامية تشكل شبكة مستقلة من مجموعة من المجرمين يقومون بارتكاب جرائم القتل"، واستمرار بقاء هذه الشبكة مرهون بارتباط أعضائها بالسكان وبالدولة بعلاقات تتنوع بين الحماية، والترويع، والرشوة[1].

وفي تعريف آخر جاء به الأستاذ GASSIN أن الجريمة المنظمة هي: "تلك الجريمة التي يمتاز التخطيط لها وارتكابها بتنظيم ممنهج، وتوفر لمرتكبيها وسائل العيش"، كما يميز بين أربعة أنواع من الجريمة المنظمة[2]:

1 ــ جريمة منظمة ذات طابع وحشي أو عنيف؛ كالخطف، والابتزاز، والسطو، والقتل..

2 ــ جريمة منظمة تتسم بالذكاء؛ كالاحتيال والنصب، الغش المعلوماتي، التزييف والتزوير، السرقة المنظمة للسيارات..

3 ــ جريمة منظمة تستغل الإغراء؛ كالدعارة، الاتجار في المخدرات، الألعاب غير المشروعة قانونا..

4 ــ جريمة منظمة تمس بالاقتصاد القومي أو الدولي، وتعرف بجرائم ذوي الياقات البيضاء white collar crime .

الفرع الثالث: مفهوم الجريمة المنظمة في القوانين الوضعية.

تتفادى أغلب التشريعات الجنائية التعريف الكافي للجريمة المنظمة خشية المساس بحقوق الإنسان والقيم الديمقراطية[3]، فنجد التشريع الفرنسي على سبيل المثال تطرق في أكثر من موضع للجريمة المنظمة خاصة ما يتعلق بسلسلة قوانين مكافحة غسل الأموال، حيث تم توسيع الالتزام بالإبلاغ عن العمليات المالية المشبوهة في عام 1993م ليشمل الأموال المحصلة من أنشطة المنظمات الإجرامية[4]،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

لكنه لم يتطرق إلى تعريفها، بل رفض تعريفها في التعديلات المتلاحقة لقوانين مكافحة غسيل الأموال[1].

وقد عرّف المؤتمر السادس عشر للجمعية الدولية لقانون العقوبات الجريمة المنظمة بأنها: "تتمثل في أنشطة مرتكبة بواسطة منظمات محترفة ومهيكلة بصورة صارمة، هذه المنظمات تميل إلى الإجرام ولا ينطبق نموذج المجرم العادي على أعضائها. وهي ترتكب جرائم جسيمة كوسيلة للحصول على الربح المالي أو بهدف الحصول أو المحافظة أو توسيع سلطاتها، أو بهدف ممارسة تأثير اقتصادي أو بهدف استغلال الأشخاص".[2]

كما عرّفت الجماعة الإجرامية المنظمة بأنها "جماعة محددة البنية، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتقوم معا بفعل مدبر بهدف ارتكاب واحد أو أكثر من الجرائم الخطيرة أو الجرائم المقررة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى".[3]

المطلب الثاني: خصائص الجريمة المنظمة.

تختلف الجريمة المنظمة عن باقي الجرائم بمجموعة من الخصائص أبرزها:

الفرع الأول: التنظيم الهيكلي المتدرج.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

فالجريمة المنظمة تبنى وفق أدوار محددة توزع على كل عضو منها، كما تختلف المنظمات الإجرامية من حيث التنظيم والهيكلة، فنجدها تتنوع من جماعات تعتمد على هيكلة هرمية ذات علاقات شبه عائلية إلى شبكات أخرى مرنة، ولقد نتج عن الهيكلة الأولى مصطلح العائلة المافيوزية La famille mafieuse كما هو معروف لدى المافيا الإيطالية؛ (الكوسا نوسترا ، الكامورا، الندرانجيتا) والتي هي في حقيقة الأمر لا تقتصر على "العائلة" بمعناها البيولوجي بل تتسع إلى كل الأعضاء الذين ينتمون لها عن طريق التحالف والتجنيد، ولقد ساهم الهيكل الهرمي في تأمين بقاء واستمرارية المنظمة، كما ساهم أيضا في إخفاء شخصية رؤساء العائلات وصعوبة القبض عليهم متلبسين بالاشتراك في الجرائم التي ينفذها الجنود. [1]

وهناك تنظيم آخر ينشط على شكل مؤسسات اقتصادية دولية واقعية، حيث تطبق طرق تقسيم العمل والمبادئ الأساسية في الإدارة كما هو معروف في عصابات الكارتل الكولومبية التي تتدخل في كافة مراحل إنتاج وتوزيع الكوكايين، أما المنظمات الإجرامية المرنة فهي تقوم على أساس الوساطة حيث تقتصر مهامها في توزيع المخدرات فقط.[2]

الفرع الثاني: قانون السرية.

إلزامية الصمت المطلق هو أحد القوانين المقدسة داخل المنظمات الإجرامية[3]، وعقاب إفشاء السر هو الموت مع إلحاق الضرر الجسيم بأسرة العضو الخائن، نظرا لما يلحقه إفشاء السر من إحداث ثغرة عميقة في الهيكل التنظيمي للمنظمة الإجرامية.[4]

الفرع الثالث: الاعتماد على وسائل غسل الأموال.

يعد غسل الأموال من أنجع وسائل إخفاء مصادر الأموال غير المشروعة المحصلة من طرف المنظمات الإجرامية كونه يصعب على الجهات الرقابية التحقق من مصدر هذه الأموال ومالكيها[5]، نظرا لسهولة دمجها في دائرة الاقتصاد المشروع حيث تستثمر في الأنشطة التجارية والاقتصادية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المشروعة التي تدر أرباحا ضخمة (كالمطاعم، والفنادق وغيرها) وبذلك تختلط الأرباح وتبدو في النهاية وكأنها نتيجة أعمال مشروعة.[1]

الفرع الرابع: استعمال العنف والرشوة لتحقيق الأهداف.

كما تعتبر الرشوة أيضا من أهم أساليب المنظمات الإجرامية بالنظر إلى ما تحققه من تأمين السيطرة على المشروعات والمؤسسات الاقتصادية والمالية، و تيسر الطريق للولوج إلى المؤسسات السياسية والإدارية والقضائية وبذلك تكسب الحصانة والحماية.[2]

أما العنف فهو تصرف يلازم كل المنظمات الإجرامية لضمان السيطرة وزيادة الثروة، ويتدرج العنف في المنظمات الإجرامية من التحذير إلى إتلاف الممتلكات وقد يصل إلى الاغتيال، وقد يوجه العنف إلى السكان كما يوجه للدولة أيضا وهو ما يحصل على سبيل المثال في إيطاليا حيث يلزم التجار والصناع بدفع مبالغ كبيرة بصفة دورية إلى المنظمة الإجرامية ليسلموا من التعرض للاعتداء والتهديد الذي يطال تجارهم أو مصانعهم.[3]

كما عاشت إيطاليا اعتداءات جسيمة اهتزت لها السلطة العامة، كاغتيالات القضاة ورجال السياسة الذين انتهجوا سياسة معادية للمافيا عن طريق إحداث تعديلات تشريعية في قانون العقوبات الإيطالي عام 1992م، الذي أقرت فيه حماية المجرمين التائبين وتجريم الاتجار في الأصوات الانتخابية، واستحداث إجراءات جنائية لمكافحة المافيا كالتفتيش ومدة التحقيق، ومركزية أجهزة التحقيق والملاحقة.[4]

المطلب الثالث: أبعاد الجريمة المنظمة في الفضاء الإلكتروني

الفرع الأول: الجريمة المنظمة والانترنت.

استطاعت الجريمة المنظمة أن تستغل الإمكانات التي تتيحها الانترنت في تخطيط وتمرير وتوجيه

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المخططات الإجرامية، وتنفيذ العمليات الإجرامية بسهولة[1]، كما نشئت من خلالها منظمات خطيرة تعمل على مستوى دولي متجاوزة بذلك الحدود الدولية معتمدة على استراتيجيات معينة وتحالفات بين المنظمات الإجرامية المحلية والخارجية لفرض السيطرة على الدول، الأمر الذي جعل هذه الظاهرة من أكبر التحديات التي تواجه الدول بكافة أشكالها وبدون تمييز بين المتقدمة منها والمتخلفة، ولقد أصبح الترابط بين الجريمة المنظمة وشبكة الانترنت يتطور بشكل مستمر نظرا لما تحققه هذه التكنولوجيا من أهداف الجريمة المنظمة في تنفيذ الجرائم وتسخير الجنود عن بعد، إضافة إلى ما تحققه من أرباح كبيرة بأقل قدر ممكن من المخاطر.[2]

أما صور الجريمة المنظمة في الفضاء الإلكتروني فهي متعددة ومترابطة مع بعض أنواع الجرائم الإلكترونية المذكورة في البحث، ولذلك سأقتصر على تجارة المخدرات باعتبارها من أبرز أنشطة المنظمات الإجرامية.

الفرع الثاني: جريمة الاتجار بالمخدرات عبر الانترنت

أشارت لجنة البلدان الأمريكية لمكافحة تعاطي المخدرات التابعة لمنظمة الدول الأمريكية في تقريرها عن نصف الكرة الأرضية لعامي 1999م و2000م، إلى أن شبكة الانترنت أصبحت تستخدم أكثر من الوسائط الأخرى في زيادة إنتاج المخدرات المصنعة واتساع رقعتها، حيث استفادة الجماعات الإجرامية المنظمة من العولمة والاتصالات الفورية والتحويلات المالية الإلكترونية في تحسين كفاءة أنشطة الاتجار بالمخدرات[3]. كما يشير تقرير صادر عن الإنتربول إلى أن 890 مليون متعاطي للمخدرات معظمهم في آسيا، وأوربا، وأمريكا الشمالية يستخدمون شبكة الإنترنت بما تتيحه من إمكانيات في الحصول على المخدرات.[4]

وقد اكتشف في سنة 2000م أكثر من 1100 موقع على شبكة الانترنت تعرض مختلف أنواع المخدرات للبيع خاصة منها مادة القنب المخدرة، إضافة إلى أنواع أخرى متفاوتة الخطورة كأقراص

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الإكستازي والكوكايين والهروين[1]، وفي تقرير نشرته شبكة CNN الإخبارية على موقعها الإلكتروني ذكرت فيه أن السلطات الاتحادية والمحلية ألقت القبض على العديد من مروجي العقار المخدر المسمى GHB عبر شبكة الانترنت[2]، كما امتدت جريمة المتاجرة بالمخدرات إلى بيع حتى المواقع الإلكترونية ذات الشهرة التجارية الكبيرة في هذا المجال بمبالغ خيالية، أو التنازل عن بريد إلكتروني يتم من خلاله الطلب أو الاشتراك في إحدى غرف المناقشة التي تقدم خدمة توزيع المخدرات وكل ذلك بمقابل مادي، وليس هذا فحسب بل توسع الأمر إلى قيام العديد من المختصين في إنتاج المواقع بتأسيس وسائط إلكترونية متكاملة كمزود لخدمات الانترنت ISP أو شبكة اتصالات متكاملة تقوم بمهمة الترويج لآفة المخدرات عبر شبكة الانترنت وعرض هذه البرامج للبيع مقابل المال.[3]

وما زاد الأمر تعقيدا ظهور كما هائلا من المواقع الإلكترونية التي تقدم شروحات تروج فيها المخدرات والمؤثرات العقلية من حيث أنواعها، وأساليب معالجتها، وكيفية تعاطيها، ووصل الأمر إلى عرض وصفات تشرح فيها كيفية صناعة المخدرات مترليا بوسائل بسيطة وبمواد أولية غير محظورة قانونا في كل بلدان العالم، حيث أشار تقرير سنوي للمجلس الدولي لمكافحة المخدرات إلى أن تعاطي مخدر القنب سجل ارتفاعا كبيرا بسبب قيام الكثير من المواقع الإلكترونية بنشر معلومات تتعلق بكيفية زراعته في المنازل، وأكد المجلس في تقريره إلى أن بذور هذا المخدر واللوازم المستخدمة في زراعته داخل المنازل يجري بيعها وتداولها عبر شبكة الإنترنت من خلال مواقع إلكترونية متخصصة.[4]

وبالرغم من التطور التكنولوجي الملحوظ لأجهزة الأمن الدولية وخبراتها الواسعة في وضع حدّ للجريمة، إلا أنّ مجرمي الانترنت لا زالوا حتى اليوم متقدّمين بخطوة على الأجهزة الأمنية، فبعد أن تدرب رجال الشرطة العالميين على مرّ السنوات في فنّ تقفي أثر تجار المخدرات ومروّجيها عبر الانترنت، فإنهم منذ عام 2011م فشلوا في القبض عليهم بسبب ابتكار المنظمات الإجرامية تقنيات أشد مكرا ودهاء للإفلات من قبضة القانون، وكمثال على ذلك أنهم أنشئوا موقعا إلكترونيا يتمتع

---

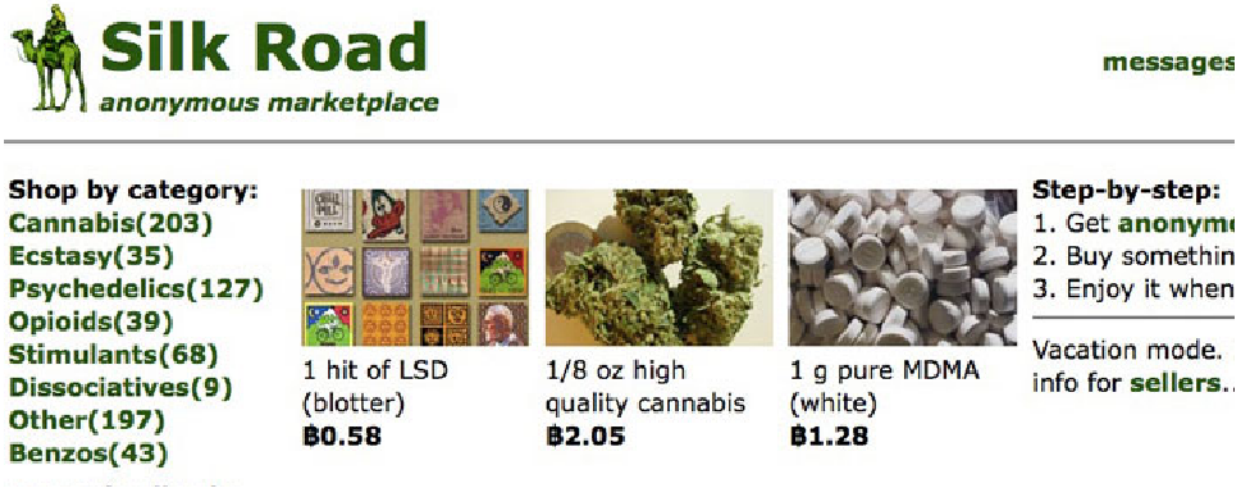
(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

بسرية فائقة مع عدم كشف هوية المتعاملين فيه، وأطلقوا عليه إسم طريق الحرير Silk Road، وهو موقع يختلف عن المواقع الأخرى إذ لا يمكن لمستخدمي الانترنت استعمال محركات البحث التقليدية مثل Chrome وFirefox للدخول إلى هذا الموقع، ولا يمكنهم أيضاً استخدام بطاقاتهم الائتمانية لشراء البضاعة، لأن عملية الدخول لا يمكن أن تتم إلا عبر محرّك TOR السرّي الذي يتطلب تنزيله خبرة عالية في مجال المعلوماتية، كما تتم فيه عمليات الشراء باستخدام عملة إلكترونية مستحدثة تسمى بـــ: Bitcoins، وهي عملة إلكترونية غير معروفة دوليا ولا تخضع لأي سلطة مصرفية أو حكومية، وهي عبارة عن عملة رقمية يتم شراؤها عبر الانترنت من دون الحاجة إلى الارتباط بإسم أو دولة، أما قيمتها فتتغير بشكل دوري ولا ترتبط بالبورصة.

كما لا يمكن تقفي أثر كل من يستخدم الموقع لأنّ محرّك TOR يخفي هوية المستخدم الالكترونية (IP address) ويحوّر مسارها، لكن مؤخرا تم اكتشاف هذا الموقع من طرف الأجهزة الأمنية المختصة وتمكنوا من توقيفه، علما أن حصّة هذه التجارة العالمية الالكترونية يفوق حجمها عشرات ملايين الدولارات[1].



شكل رقم (18) يبين الموقع الإلكتروني Silk Road لتجارة المخدرات بعد اكتشافه وتوقيفه[2]

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث: الإرهاب الإلكتروني

يعود مصطلح الإرهاب الإلكتروني إلى الثورة الهائلة التي جلبتها حضارة التقنية في عصر المعلومات، حيث شاع استخدام هذا المصطلح بعد اتساع رقعة الجرائم الإرهابية وتعقيدها سواء من حيث تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها، أو من حيث تبادل المعلومات فيما يخص الأساليب والطرق الإجرامية المبتكرة، وهو الأمر الذي استدعى استنفار العديد من الدول خاصة المتضررة منها للتوقيع على أول اتفاقية دولية لمكافحة الإجرام المعلوماتي بما فيها الإرهاب وذلك في العاصمة المجرية (بودابست) سنة 2001م.[1]

المطلب الأول: مفهوم الإرهاب الإلكتروني.

الفرع الأول: تعريف الإرهاب في اللغة والاصطلاح.

أولا: تعريف الإرهاب في اللغة: لم يظهر لفظ الإرهاب في المعاجم العربية القديمة لكنها عرفت الفعل: رهب ـــ يرهب، رهبة ورهبا، أي خاف، ورهبة ورهبا أي خافه، والرهبة هي الخوف والفزع.[2]

وورد في المعاجم المترجمة إلى اللغتين الانجليزية والفرنسية، لفظ الإرهاب بما يفيد أنه وسيلة لنشر الذعر والتخويف باستعمال وسائل عنيفة لتحقيق أهداف سياسية.[3]

كما عرّف مجمع اللغة العربية كلمة الإرهاب؛ أن مصدرها الفعل أرهب، بمعنى خوف، وأرهب بمعنى ركب الرهب، أي ما يستعمل في السفر من الإبل، وأرهب أطال كمه.[4]

وأطلق مجمع اللغة العربية في معجمه الوسيط على الإرهابيين أنه وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم[5]، فكلمة إرهاب تستخدم للرعب أو الخوف الذي يسببه فرد، أو جماعة، أو تنظيم سواء كان لأغراض سياسية أو شخصية أو غير ذلك.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثانيا: تعريف الإرهاب في الاصطلاح القانوني.

شهد مفهوم الإرهاب في القانون تعريفات مختلفة من بينها:

تعريف اتفاقية جنيف للأعمال الإرهابية سنة 1937م على أنها: "الأعمال الإجرامية الموجهة ضد دولة ما بهدف خلق حالة من الرعب في أذهان أشخاص معينين، أو مجموعة من الأشخاص، أو عامة الجمهور".[1]

كما عرف الإرهاب في المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب التي صدرت بالقاهرة عام 1998م، بأنه: "كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إفشاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر"[2].

ويعرّف أيضا أنه: "استخدام غير شرعي للقوة أو العنف أو التهديد باستخدامها بقصد تحقيق أهداف سياسية".[3]

ومن التعريفات الحديثة للإرهاب أنه: "نوعا من استخدام الطرق العنيفة كوسيلة، الهدف منها نشر الرعب في المجتمع لإضعاف الحكم وتحقيق تغيرات سياسية".[4]

الفرع الثاني: مفهوم الإرهاب عند مجامع الفقه الإسلامي.

عرّف مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي، الإرهاب بأنه: "العدوان الذي يمارسه أفراد أو جماعات أو دول بغيًا على دين الإنسان، ودمه، وعقله، وماله، وعرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصور الحرابة، وإخافة السبيل، وقطع الطريق، وكل فعل من أفعال العنف أو التهديد يقع تنفيذًا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ومن صنوفه إلحاق الضرر بالبيئة أو المرافق العامة والأملاك الخاصة أو الموارد الطبيعية، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها[1] .[2]

وفي قرار صادر من مجمع الفقه الإسلامي الدولي في دورته الرابعة عشرة المنعقدة في الدوحة في شهر ذي القعدة من عام 1423هـ ذكر فيه تعريف مصطلح الإرهاب بأنه: "العدوان أو التخويف أو التهديد ماديًا أو معنويًا الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه، أو نفسه أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض"[3].

الفرع الثالث: تعريف الإرهاب الإلكتروني

لا يكاد يختلف مفهوم الإرهاب الإلكتروني عن مجموعة المفاهيم التقليدية له، وإنما يختلف عنها في طرق التنفيذ التي تعتمد الوسائل التكنولوجية الحديثة بالإضافة إلى استهدافه للبيئة الرقمية في حد ذاتها، وكنتيجة لذلك يعرّف الإرهاب الإلكتروني بأنه: " جريمة العدوان أو التخويف أو التهديد المادي أو المعنوي باستخدام الوسائل الإلكترونية، وسواء كان هذا التهديد صادرا من الدول أو الجماعات أو الأفراد بهدف إلحاق شتى صنوف الضرر بالإنسان في دينه أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق" [4].

وهو تعريف يبين أن صور الجرائم التي ينطوي عليها مفهوم الإرهاب الإلكتروني ـــ كجريمة إلكترونية ـــ أنها تستهدف المعطيات بأنواعها كمحل للجريمة، أو تستخدم التكنولوجيا لارتكاب جرائم تمس الأموال والأشخاص وكل ما له علاقة بعمل الأجهزة الحكومية، كما تستهدف عبر السيطرة على نظم المعلومات الترويع ونزع الثقة بنظم التقنية، ولعل الصورة الواضحة للإرهاب الإلكتروني ما أصبح يعرف بحرب المعلومات الشاملة التي تستهدف كل نظم ومعطيات الأنشطة الحيوية والإستراتيجية لأي دولة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثاني: خصائص الإرهاب الإلكتروني وأهدافه.

الفرع الأول: خصائص الإرهاب الإلكتروني.

يتسم الإرهاب الإلكتروني بعددٍ من الخصائص يختلف فيها عن بقية الجرائم، ومن أهمها ما يلي:

1. يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية تتعدى الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود.
2. يصعب اكتشاف جرائم الإرهاب الإلكتروني، الذي يقابله نقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.
3. كما يصعب إثبات جرائم الإرهاب الإلكتروني نظراً لصعوبة تقفي الدليل الرقمي وسهولة إتلافه وتدميره.
4. من خصائص مجرمي الإرهاب الإلكتروني أنهم من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل لديهم قدرات من المعرفة والخبرة في التعامل مع الحاسوب والشبكة المعلوماتية.

الفرع الثاني: أهداف الإرهاب الإلكتروني.

يسعى الإرهاب بعمومه ـــ التقليدي والإلكتروني ـــ إلى تحقيق جملة من الأهداف غير المشروعة وبيان أهمها كما يلي:

1 ـــ نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة.

2 ـــ الإخلال بالنظام العام، والأمن الاجتماعي، وزعزعة الطمأنينة.

3 ـــ تعريض سلامة المجتمع وأمنه للخطر.

4 ـــ إلحاق الضرر بالبنى المعلوماتية الأساسية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة.

5 ـــ تهديد السلطات العامة والمنظمات الدولية وابتزازها.

6 ـــ الانتقام من الخصوم حتى وإن كان على حساب مجتمع كامل.

7 ـــ الدعاية والإعلان، وجذب الانتباه، وإثارة الرأي العام.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

9 ــ العمل على تقويض النظام السياسي في الدول.

10 ــ تدمير المنشآت الحيوية، والمرافق العامة.[1]

المطلب الثالث: صور الإرهاب الإلكتروني.

إن المتعقب لصور الإرهاب الإلكتروني المتعددة ــ كجريمة إلكترونية ــ يجدها تستهدف المعلومات بأنواعها كمحل للجريمة حيث صنفت العديد من الجرائم الإلكترونية ضمن قائمة الإرهاب الإلكتروني بالنظر إلى ما تؤول إليه من مخاطر جسيمة كالتجسس الإلكتروني، ونشر الفيروسات، واختراق البريد الإلكتروني، وتعطيل الأنظمة الإلكترونية وغيرها، وفي الغالب يستند السلوك الإجرامي للإرهاب الإلكتروني إلى دوافع سياسية ضد المعطيات بأنواعها ونظم وبرامج الكومبيوتر والاتصالات من أجل تحقيق أغراض إرهابية تنطوي على عنف يستهدف حياة الأفراد وسلامتهم وإثارة الفوضى وإشاعة الخوف وتعطيل الأداء الطبيعي لنظم السيطرة والرقابة الإلكترونية، وتعطيل عمل الأجهزة والهيئات الحكومية والمرافق الاستراتيجية في الدولة، ومن أخطر صوره ما يلي:

الفرع الأول: نشر مواقع ثقافة التطرف المفضي إلى العنف والإرهاب.

ثبت أن الجماعات المتطرفة كانت من الأوائل التي استخدمت العالم الإلكتروني في نشر أفكارها وذلك قبل ظهور شبكة الانترنت، حيث أشارت مصادر غربية أن "توم ميتزقر" Tom Metzger أحد أشهر المتطرفين الأمريكيين العنصريين ومؤسس مجموعة "المقاومة الأريانية البيضاء" White Aryan Resistance كان من أوائل من أسس مجموعة بريد الكترونية ليتواصل مع أتباعه سنة 1985م[2]. كما عرفت جماعات كثيرة عبر شبكات المعلومات ما قبل الشبكة العالمية كجماعة المتطرف الأمريكي "دان جانوون" Dan Gannon الذي يعد بحسب المصادر الغربية[3] أول من أنشأ موقعا متطرفا يدعو إلى الفكر العنصري عن نقاء العرق الأبيض، ومع ولادة الانترنت في الولايات المتحدة الأمريكية ظهرت عدة مجموعات متطرفة أشهرها مجموعة "جبهة العاصفة" Stormfront الأمريكية المسيحية التي كان

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المصورة.

...../...

يقودها "دون بلاك" Don Black التي أنشأت أول موقع شامل يدعو إلى ثقافة الكراهية والتمييز العنصري سنة 1995م، وتلى ذلك ظهور العديد من المواقع التابعة لجماعات متطرفة من الولايات المتحدة وأروبا وبشكل خاص بريطانيا واستراليا ثم بقية دول العالم.[1]

كما أسهمت أيضا الانترنت في العالم الإسلامي في بسط نفوذ التطرف الفكري لمختلف التيارات وذلك من خلال المواقع والمنتديات التي تديرها جماعات ورموز متطرفة، حيث تقدم منتجاتها الفكرية وفق خطاب جذاب مستغلين الحس الديني البريء لدى الشباب لتضخ فيه الأفكار المضللة وتزين لهم أفكار الخروج عن المجتمع والهجرة عن الأوطان موظفة بعض مظاهر الإحباط السياسي والاقتصادي والاجتماعي لتوجيه طاقات هؤلاء الشباب إلى محاربة مجتمعاتهم وتكفير حكامهم وقتل أنفسهم في سبيل ما يعتنقون من أفكار مزعومة. ويتم غرس القناعات الفكرية التي تتبناها وتروجها تنظيمات التطرف وفق مراحل تنشئة فكرية اجتماعية يتم من خلالها إدماج الفرد في مجتمع الصفوة الجديد بتعزيز قيم ومعايير وقواعد معنوية ومادية جديدة ليكتمل البناء الفكري للحصول على نوعية الفرد الذي يريدون، ومن ثم تشكيل الاتجاهات الاجتماعية التي يرغب المجتمع الجديد نقلها له من خلال إشباع حاجاته الأساسية خاصة الحاجة للأمن والتقدير والحاجة للانتماء وهي مهمة بعد العزل الشعوري واللاشعوري عن محيطه القديم، وبشكل عام يمكن رصد هذا التدرج من خلال منظومة متكاملة على النحو التالي:

ـــ بناء منظومة من القناعات الفكرية حول المجتمع والسياسة والحكم والحياة.

ـــ التشكيك ونقد القناعات المستقرة عند الناس خاصة في الجانب السياسي بتوظيف ديني.

ـــ التباهي بمجتمع الصفوة الجديد الذي ينتمون إليه مع ذم المجتمع الغارق في شهواته وجهله وتنفير الشباب من هذه المجتمعات.

ـــ تشويه سيرة العلماء والدعاة من خارج الفكر وتتبع عثراتهم واتهامهم بمداهنة السلطات وبيع الذمة.

ـــ تمجيد أسماء وسير شخصيات معاصرة وتاريخية وانتقاء ما يتناسب من مواقفها وآرائها لدعم وتعزيز الخط الفكري والعسكري لهذه التنظيمات.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

ـــ نسف الأفكار الوسطية وبناء أساس فقهي جديد يعتمد على الأفكار المتشددة كبديل وترويجه بين الشباب باستثمار حماسهم وقلة معرفتهم الشرعية.

ـــ هدم الرموز الفكرية التي اعتاد الناس التوجه لها كمراجع في مختلف القضايا وإعلاء أسماء رموز الفكر المتطرف كبديل نزيه في عالم يسوده الظلم والخيانة.

ـــ الاغتيال المعنوي للرموز السياسية واتهامهم بالعمالة والمداهنة والطغيان.

ـــ إعلان إنشاء كيانات سياسية وتسمية أمراء ودول، وعقد تحالفات وإعلان الحرب مثلما هو حاصل في العراق.

ـــ الاندساس بين ذوي التقاليد القبلية والمحافظة لاستغلال ما يرونه أخطاء في التظاهرات الثقافية وغيرها ورفع صوت الاحتجاج وإثارة العامة. [1]

ومن سمات هذه المواقع أنها تروج للتطرف وثقافته بتتبع الأحداث التي تخدم معتقداتهم فيختارون عناوين مشحونة بالشجن والدفق العاطفي كذكر "الثواب" و"الجنة" و "الحور العين" ونحو ذلك، وبصفة عامة يمكن تعداد مجموعة من السمات المشتركة بين هذه المواقع على النحو الآتي: [2]

ـــ الشكل الفني المبدع في التصميم والحرفية الواضحة في تقسيم الموضوعات والصور والمحتويات.

ـــ توفير خدمات تجاوز حجب المواقع وترسل بصورة منتظمة للأعضاء وتقدم كل جديد من خلال التواصل المنتظم مع الأعضاء.

ـــ التحديث المستمر للمحتوى ومواكبة الأحداث وملامسة رد الفعل الإنساني العفوي للمسلم تجاه الشعوب الإسلامية والتعليق عليها وفق وجهة النظر التي يؤمنون بها.

ـــ استقطاب مؤلفين لهم تأثيرهم والنشر لعلماء معتبرين لرفع مستوى الثقة في الموقع.

ـــ التنسيق العالي بين هذه المواقع لنشر البيانات والخطب والمواد الجديدة التي يقدمها أحد قادة التنظيمات أو مفكريها.

ـــ صناعة نجوم لهذه المنتديات ومؤازرتهم سواء من حيث حجم الردود أو تمييز مواضيعهم عن غيرها.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ توفير المواد السمعية والبصرية والكتب وغيرها من المواد لطالبيها بشكل سريع وفي صور فنية احترافية.

ـــ تشجيع كتابة المذكرات للذين شاركوا في "الحرب" في مناطق العالم الإسلامي مثل أفغانستان والعراق لإلهام المتلقين وتحفيزهم للاقتداء بهؤلاء باعتبارهم "أبطال".

ـــ تقديم المعونة الفنية لمساعدة المتصفحين لإخفاء الأثر من خلال مواقع وسيطة أو برامج معينة.

ـــ توزيع الأدوار في إدارة الموقع (المشرفين) لأشخاص ذوي كفاءة متميزة وينتمون إلى بلدان مختلفة.

ـــ تقديم باقة من الخيارات الثقافية المصاحبة كخدمة تحميل الكتب الإلكترونية والاستشارات في شؤون الأسرة والفتاوى والصحة وغيرها..

الفرع الثاني: المتاجرة غير المشروعة بالأسلحة عبر الانترنت

تعد تجارة الأسلحة ثاني أكبر دخل بعد المخدرات ضمن التجارة الممنوعة دولياً ، كونهما يندرجان تحت جريمة غسيل المال والإرهاب، ولقد أخذت هذه التجارة أسلوباً حديثا لترويجها في بلدان العالم عبر المواقع الإلكترونية خاصة منها صفحات التواصل الاجتماعية، وذلك عن طريق عرض صورة السلاح ومعلومات تفصيلية عنه، بالإضافة إلى توضيح طرق التواصل .

وعلى سبيل المثال جاء في تقرير حول تجارة الأسلحة بليبيا نشرته يومية العرب[1] ، أنه في ظل تطور تجارة السلاح، شرعت جماعات إرهابية في ممارسة هذه التجارة عبر مواقع التواصل الاجتماعي، كما استحدث تجار الأسلحة في ليبيا ـــ على وجه الخصوص ـــ نمطا جديدا لإبرام صفقات البيع والشراء، حيث قاموا بنشر إعلانات لبيع وشراء الأسلحة على صفحة خاصة أنشئت على موقع الفيسبوك، كما تستعمل مجموعات أخرى الفيسبوك بهدف التواصل بين بائعي الأسلحة والراغبين في شرائها أو مبادلتها.

وفي تقرير نشرته قناة العربية الفضائية على موقعها الإلكتروني[2]، "أنه من خلال معاينة أحد الصفحات التي زاد عدد المعجبين بها عن عشرة آلاف معجب نلاحظ حماسا وإقبالا شديدا على اقتناء

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

الأسلحة من قبل المواطنين باختلاف جنسياتهم، ويبيع صاحب الصفحة المشار إليها الأسلحة الخفيفة على غرار المسدسات وأسلحة الكلاشنكوف بالإضافة إلى البدلات العسكرية والمعدات اللوجستيكية".

شكل رقم (19):يظهر سوق افتراضية للأسلحة على موقع التواصل الاجتماعي الشهير "فايس بوك " يعرضها أحد الباعة الليبيين لعامة الناس، وقد بلغ عدد الذين أعجبهم الموقع في فترة وجيزة 10596 مطّلع[1].

الفرع الثالث: آثار تجارة الأسلحة على الأفراد والمجتمعات

تكلّف التجارة غير المشروعة للأسلحة مضارا بالغة على البشرية؛ فكل يوم يتعرض آلاف البشر للقتل أو الإصابة أو الاغتصاب، كما يجبر العديد من الفرار من ديارهم نتيجة العنف المسلح وانتهاكات حقوق الإنسان[2]، وقد جاء في تقرير عالمي حول عدد القتلى جراء النـــزاعات المسلحة التي تم الإبلاغ عنها خلال السنوات 2004م إلى غالية 2007م، أنه تم تسجيل ما لا يقل عن 208300 وفاة ناجمة عن عنف النـــزاعات المسلحة، أي بمعدل 52000 شخص كل سنة.[3]

كما يتسبب النـــزاع المسلح في وفيات غير مباشرة لأن الحروب كثير ما تؤدي إلى التهجير، ويعرِّض البنية التحتية الاجتماعية والاقتصادية للدمار، ويحرم الناس من الحصول على الرعاية الصحية والماء والغذاء والمأوى، ويؤدي بالنتيجة إلى رفع معدلات سوء التغذية والموت جوعاً وغيرها من

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الآفات التي يمكن الحيلولة دونها. وتشير الشواهد التي خلصت إليها الدراسات المسحية الخاصة بالأوبئة إلى أن ما لا يقل عن 200000 وفاة غير مباشرة نجمت عن النـــزاعات المسلحة كل سنة، وربما أكثر بكثير، ما بين 2004م و2007م. [1]

أما خارج النزاعات المسلحة التي تشمل أعمال القتل المسلح دون سابق ترصد وغير ذلك من أشكال الجريمة المسلحة، وعمليات الإعدام خارج نطاق القضاء والقتل غير القانوني الناجم عن الاستخدام المفرط للقوة، وأعمال القتل الناجمة عن العنف ضد النساء وغيرهن من الفئات المستضعفة باستعمال الأسلحة أو عبر التهديد بها، فقد سجل ما يقدر بنحو 290000 عملية قتل كل سنة خارج النـــزاعات على نطاق العالم بأسره في السنوات الأخيرة، بينها ما معدله 60% استخدمت فيه الأسلحة النارية.[2]

كما أدى استخدام الأسلحة إلى تفاقم آلاف الانتهاكات والإساءات لحقوق الإنسان كل عام، وعلى رأسها التعذيب والاغتصاب، حيث بينت أبحاث مفصّلة تناولت عينة مركبة من 10 بلدان أن 60% من جميع الحالات الفردية لانتهاكات حقوق الإنسان والإساءة إليها التي قامت منظمة العفو الدولية بتوثيقها ما بين 1991م و2002م، سواء في سياق النـــزاع المسلح أم خارجه، انطوت على استخدام مباشر للأسلحة الصغيرة والأسلحة الخفيفة.[3]

وقد أدى توافر السلاح على نطاق واسع وفوضوي إلى انتهاكات وإساءات جماعية لحقوق الإنسان والتي شملت ما يلي:

ـــ تجنيد الأطفال: حيث يشير التقرير أن آلاف الأطفال كانوا ما بين أفريل 2004م وأكتوبر 2007م يشاركون في نزاعات مسلحة في 19 دولة ومنطقة على نحو نشط في جميع أنحاء العالم، سواء في صفوف القوات الحكومية أو مع الجماعات المسلحة المعادية، بما يعنيه ذلك من أضرار لحقت بسلامتهم النفسية والعقلية.[4]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ انتهاكات أدت إلى تهجير الأشخاص والمجتمعات: إذ قدَّرت المفوضية العليا للاجئين التابعة للأمم المتحدة سنة 2008م أن عدد من هجِّروا داخلياً نتيجة للنـــزاع المسلح على نطاق العالم بأسره بلغو نحو 26 مليون شخص، وهو رقم تزايد على مدار سنوات العقد الأخير[1] ، وغالباً ما يسهم التهجير في الحرمان من الحقوق المدنية والسياسية والاقتصادية والاجتماعية والثقافية.

وبالإضافة إلى ذلك، فقد فرَّ العديد من اللاجئين الذين يقدر عددهم على مستوى العالم بأسره نحو 15.2 مليون لاجئ هرباً بأنفسهم من انتهاكات حقوق الإنسان التي زاد العنف المسلح من خطورتها، وتجدر الإشارة إلى أن جميع الدول التي كانت على رأس قائمة البلدان المصدرة للاجئين في سنة 2008م هي دول تدور فيها نزاعات مسلحة، ومن بينها: العراق، والصومال، والسودان، وكولومبيا، وجمهورية الكونغو الديمقراطية، وأفغانستان، وتقدر المفوضية العليا للاجئين أن أفغانستان وحدها تشكل في الوقت الراهن مصدر ربع إجمالي اللاجئين على نطاق العالم بأسره.[2]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الباب الثالث

الآليات الفنية والتشريعات القانونية لمكافحة الجريمة الإلكترونية

الفصل الأول: الإجراءات الفنية لمكافحة الجريمة الإلكترونية

الفصل الثاني: التدابير والتشريعات القانونية لمكافحة الجريمة الإلكترونية

1)
2)
..

تمهيد:

على ضوء التطورات المتسارعة للجرائم المستحدثة التي أصبحت من أكبر السلبيات التي خلفتها الثورة المعلوماتية، حيث شملت اعتداءاتها قيما جوهرية تخص الأفراد والمؤسسات وحتى الدول في كافة نواحي الحياة، كما تركت في النفوس شعورا بعدم الثقة بخصوص التعامل والاستفادة من ثمار هذه الثورة الجديدة، فقد أضحى التعامل بالأدلة الرقمية يترافق مع تحديات كبيرة ويتطلّب إجراءات محدّدة للحفاظ على سلامة المعلومات وتجنّب تعديل الأدلة أو حذفها أو التعدي على حقوق مستخدمي الانترنت، ومن بين التحديات الأساسية؛ صعوبة كشف أدوات الجرائم الإلكترونية التي يستخدمها المشتبه بهم، كما يصعب كشف هوية مستخدمي الانترنت عن طريق تحليل الرسائل الالكترونية أوتحديد الأدلة ذات الصلة بالجرائم وفك تشفير الملفات، ومن ناحية أخرى فإن ظاهرة الجريمة الإلكترونية تطرح تحديات قانونية تتعلق بسيادة الدول وصلاحية محاكمها التي لا تتعدى مساحتها الجغرافية، وهو ما يستلزم تنسيقًا كبيرًا بين القوانين الداخلية والمعاهدات الدولية والتعاون بين مختلف البلدان.

وأمام هذا الوضع المقلق أدى بالمجتمع الدولي إلى التفكير الجاد في تحديد الأساليب الأمنية والإجراءات الدفاعية والتدابير الوقائية لحماية المنظومة المعلوماتية من التعدي الإلكتروني، وهو ما سأتطرق إليه في الفصول التالية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الأول:
الإجراءات الفنية لمكافحة الجريمة الإلكترونية

المبحث الأول: مفهوم أمن المعلومات

المبحث الثاني: الوسائل التقنية لأمن المعلومات

المبحث الثالث: الجاسوب الجنائي ودوره في أمن المعلومات

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: مفهوم أمن المعلومات Information Security

من المسلم به أن للتقنيات الجديدة محاسنها ومساوئها، وتجاوبا مع الحاجة لدرء أخطار أمن المعلومات فإن نشاط البحث والتطوير في هذا المجال ينمو بشكل يكاد يفوق أنشطة البحث والتطوير في مجالات حقل تقنية المعلومات والاتصالات، وقد يتوقع أن يصبح موضوع أمن المعلومات فرعا مستقلا من فروع المعرفة الإنسانية حاله في ذلك حال بعض العلوم التي تبدأ كممارسات متفرقة ثم تأخذ شكل علم أو فرع من علم مستقل.

المطلب الأول: مفهوم أمن المعلومات.

لقد عرف مفهوم أمن المعلومات تعريفات عديدة تتقارب كلها من حيث الأهداف المنشودة، ومن أهمها ما يلي:

يعرّف أمن المعلومات بأنه مجموعة من الإجراءات و التدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات، إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال [1].

كما يعرّف على أنه الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع والتلف أو من مخاطر الاستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية[2].

ويعرّف أيضا بأنه مجموعة من التدابير الوقائية المستخدمة في المجالين الإداري و الفني لحماية مصادر البيانات من أجهزة وبرمجيات وبيانات من التجاوزات أو التداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلسل أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية، فضلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التي تؤدي إلى فقدان بعض المصادر كلاً أو جزءاً، و من ثم التأثير على نوع ومستوى الخدمة المقدمة[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وهو أيضا العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها [1].

وما نستنتجه من هذه التعريفات أن مفهوم أمن المعلومات هو ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزونة في أجهزة الحاسوب إضافة إلى الأجهزة الملحقة و شبكات الاتصالات، والتصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزونة أو التي ترمي إلى نقل أو تغيير أو تخريب المخزون المعلوماتي لهذه القواعد.

المطلب الثاني: المهام الرئيسية لأمن المعلومات

إضافة إلى المهام التي أبرزتها التعريفات المتعلقة بأمن المعلومات فإنه بالإمكان تحديد المهام الرئيسية كما يلي:[2]

أولا ــ تصنيف المعلومات: وهي عملية أساسية تهتم بتصنيف المعلومات Information classification إلى معلومات متاحة، وموثوقة، وسرية، وسرية للغاية أو قد تكون معلومات متاحة الوصول إليها وأخرى محظورة التوصل إليها وهكذا.

ثانيا ــ التوثيق Documentation : ويتعلق الأمر بعملية التوثيق الخطي لبناء النظم التطبيقية المعتمدة وكافة وسائل المعالجة والتبادل، ففي الإطار الأمني يستوجب توثيق السياسة الأمنية وإجراءاتها ومكوناتها، إضافة إلى خطط التعامل مع المخاطر والحوادث والجهات المسئولة ومسؤولياتها وخطط التعافي وإدارة الأزمات، وخطط الطوارئ المرتبطة بالنظم عند حدوث الخطر.

ثالثا ــ التحسيس بالواجبات الإدارية والشخصية: يتوقف نجاح الواجبات الإدارية أو الجماعية للمؤسسات على إدراك كافة المعنيين في الإدارة ــ بمهامهم التقنية والإدارية والمالية ــ إضافة إلى أهمية الإلمام بالخطة الأمنية واستراتجياتها، وهذا ليتسنى للجميع معرفة مسؤولياتهم الأمنية تجاه المؤسسة.

رابعا ــ توفير وسائل التعرف وتصريحات الاستخدام: وهو ما يعرف بأنظمة التعرف والتصريح Identification and Authorization Systems والتي عن طريقها يمكن الوصول إلى المعلومات أو

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

الخدمات في قطاعات استخدام النظم أو الشبكات أو قطاعات الأعمال الإلكترونية، ومن بين هذه الوسائل؛ كلمات المرور والأرقام والرموز السرية التي يعرفها المستخدم، أو بصمة الأصبع أو بصمة العين والصوت وغيرها، لكن أيا كانت وسيلة التعرف المتبعة فإنها تخضع أيضا لنظام أمن وإرشادات أمنية يتعين مراعاتها، فعلى سبيل المثال كلمات المرور السرية تخضع لسياسة مدروسة كعدد مكوناتها وابتعادها عن الكلمات السهلة التخمين إضافة إلى وجوب الحفاظ عليها، فإذا تحقق ذلك فإن المرحلة التي تليها هي تحديد نطاق الاستخدام Athorization بمعنى مدى إتاحة وسيلة الدخول لاستعمال النظام من حيث التحكم أو الوصول إلى المعلومات أو أجزاء منها وهو ما يعرف بـــ Access Control System.

خامسا ـــ سجل الأداء: وهي سجلات الكترونية مهمتها التعرف على شخص المستخدم ووقت الاستخدام، ومكانه وطبيعة الاستخدام أو أي معلومات إضافية أخرى صادرة من النشاط ذاته، حيث توثق كل العمليات التي يتم فيها استخدام الجهاز وبرامجه والنفاذ إليها، كما تتباين من حيث نوعها وطبيعتها وغرضها إلى سجلات الأداء التاريخية والسجلات المؤقتة، وسجلات التبادل، وسجلات النظام، وسجلات الأمن، وسجلات قواعد البيانات والتطبيقات، وسجلات الصيانة أو ما يعرف بسجل الأدوات التقنية وغيرها.

سادسا ـــ توفير عمليات الحفظ Back-up: وهي من المهام الأمنية التي تتيح إمكانية النسخ الاحتياطي للمواد المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه، حيث تتم وفق قواعد تكون محددة سلفا وموثقة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية.

سابعا ـــ توفير وسائل الأمن التقنية: وهي أحد المهام الرئيسية لأمن المعلومات ممثلة في التقنية المبتكرة لمواجهة المخاطر المضرة بالبيئة الإلكترونية، كالجدران النارية Firewalls، والتشفير Cruptography، وكذا نظم التحكم في الدخول، ونظم كشف الاختراقات Intrusion Detection Systems (IDS)، وبرامج مقاومة الفيروسات وغيرها.

ثامنا ـــ توفير نظام التعامل مع الحوادث: وهو من المطالب الرئيسية بالنسبة لمؤسسات الأعمال خاصة المالية منها، فالتعامل مع الحوادث هي عملية متكاملة تتصل بأداء تسلسلي خاضع لقواعد

(1) الإحالات في النسخة المطبوعة.
(2) الإحالات في النسخة المطبوعة.

.../.....

محددة سلفا تستوجب تنفيذها في دقة وانضباط، وتختلف مكونات ومراحل خطوات التعامل مع الحوادث من مؤسسة إلى أخرى وذلك حسب طبيعة الأخطار المتوقعة وفق إستراتيجية الأمن المسطرة في المؤسسة، وتبعا للنظام محل الحماية كقواعد بيانات أو شبكات أو مزيج منها، إذ تختلف خطوات التعامل مع الحوادث لدى بنوك الانترنت مثلا عنها لدى المواقع المعلوماتية، لكن تتحد نظم التعامل مع الحوادث في أنها تتقاطع في ستة مراحل رئيسية وهي: مرحلة الإعداد المسبق، ومرحلة التحري والملاحظة، ومرحلة الاحتواء والاستئصال، ومرحلة التعافي والعودة للوضع الطبيعي، والمرحلة النهائية هي مرحلة المتابعة لعدم تكرار الحادثة.[1]

المبحث الثاني: الوسائل التقنية لأمن المعلومات

لقد أدى تفشي ظاهرة الاعتداءات الإلكترونية إلى بروز سوق تقنية المعلومات المتخصصة، حيث نشأت شركات عملاقة تعمل في حقل أمن المعلومات ووسائله وحلوله، كما اتجهت أيضا الدراسات البحثية والإستراتيجية والعلمية وحتى القانونية إلى التعامل مع وسائل الأمن على استقلالية، وقد نتج عن ذلك ظهور برامج لها دور أمني فعال في التصدي وإضعاف الاعتداءات الإلكترونية كالبرامج المضادة للفيروسات، وبرامج التشفير، وبرامج التعريف والتحكم في الدخول إلى الأنظمة وغيرها.

المطلب الأول: البرامج المضادة للفيروسات

الفرع الأول: مفهوم البرامج المضادة للفيروسات

سبق التطرق إلى الفيروسات بأنها برامج حاسوبية خبيثة تنتج لأغراض تخريبية عديدة كإلحاق الأضرار بالحواسيب وأنظمتها، وهي تختلف من حيث تنفيذ نشاطها فهنالك من يبدأ بتاريخ أو وقت محدد ومنها من يبدأ بالعمل بعد تنفيذ أمر معين في البرنامج المصاب، ومن الفيروسات من يبدأ بالنشاط بعد التكاثر والوصول إلى عدد معين من النسخ[2]، ومن خصائصها؛ سرعة الانتشار، والقدرة

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

على التخفي إلى درجة أن بعض البرامج المضادة للفيروسات لا تستطيع ملاحظتها، كما تتميز بالقدرة التدميرية كأن ينشطر الفيروس ليخرب أكبر عدد ممكن من الحواسيب على مستوى العالم كما أحدثه فيروس تشرنوبل الشهير Chernobyl Virus .[1]

والبرامج المضادة للفيروسات هي أحد الوسائل التقنية المحافظة على أمن المعلومات، فهي تعمل على مسح ورصد البرامج المشبوهة التي تتميز بخصائص معينة أو تحتوي على صيغة معينة من البرمجة الخاصة بلغة الكمبيوتر[2]، كما تقوم هذه البرامج بحماية الحواسيب من هجمات الفيروسات وكل ما يشكل تهديدا أمنيا على المعلومات، وبفضلها يمكن التعرف على الملفات الضارة المتسللة من أي مصدر كان، كالأقراص المدمجة وشرائح الذاكرة و الرسائل الإلكترونية، كما يمكنها اكتشاف البرامج الخبيثة على الأقراص الصلبة أو الشبكات والقضاء عليها.

الفرع الثاني: طرق عمل البرامج المضادة للفيروسات

يقوم البرنامج المضاد للفيروسات بتحليل كل الملفات والبرامج ذات الطبيعة التنفيذية، ثم تتم مقارنة التوقيع الموجود على كل ملف بالتواقيع المخزنة في قاعدة المعلومات الخاصة بالبرنامج، علما أن كل برنامج مضاد للفيروسات باستطاعته التعرف على أكثر من 40000 نوع من الفيروسات، وأكثر من عشرة آلاف نوع من تواقيع أحصنة طروادة و الديدان، كما تتيح كل شركة منتجة للبرامج المضادة للفيروسات لمستخدمي برامجها التحديث التلقائي حيث يتم فيه إضافة ميزة التعرف على الفيروسات التي ظهرت حديثا، وبعد عملية المقارنة يقوم البرنامج المضاد باكتشاف الفيروس أو حصان طروادة فيقوم بإنذار المستخدم عنه ويخيره بين مسح أو تعطيل الفيروس أو التكفل به بطريقة آلية[3].

وبالرغم من أن هذه البرامج تحمي الأجهزة من مخاطر الفيروسات إلا أنه يعاب عليها عدم قيامها بالتصحيح الشامل لنقاط الضعف المتعلقة بالمنافذ والمعابر الموجودة في الأجهزة التي يتمكن المخترقين من خلالها الوصول إلى المعلومات الخاصة، ومن أشهر هذه البرامج استخداما؛ **Bitdefender**

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

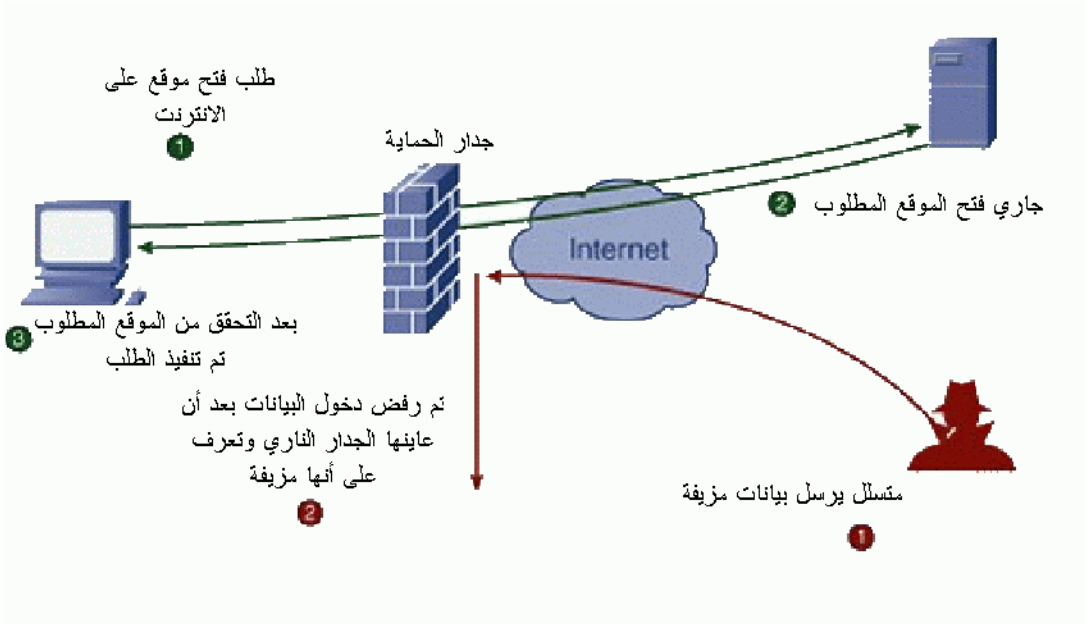
...../...

Antivirus، Avast Antivirus، AVG Antivirus ، Norton Antivirus، Kaspersky Antivirus ، McAfee Antivirus .

المطلب الثاني: الجدران النارية Firewalls.

هي من الأدوات الأمنية الفعالة المعروفة بجدران الحماية حيث تتحدد مهامها الأساسية في منع مرور البيانات الغير مرغوب فيها بين الشبكة الداخلية المحمية والشبكة الخارجية، وذلك وفق سياسة أمنية معينة كأن تمنع البيانات الدخيلة من وصولها إلى الأجهزة المحمية بينما تسمح بخروج البيانات من الداخل إلى الخارج، أو قد تسمح هذه السياسة بالدخول إلى أماكن معينة فقط دون غيرها، أو تسمح لمستخدمين معينين باستعمال بعض البيانات دون الباقي.

وقد تكون جدران الحماية على شكل برامج تطبيقية Software — Application Gateways — تثبّت على الحواسيب، كما تكون أيضا في شكل أجهزة مادية Hardware ، ومن مهامها أيضا منع المتسللين والعديد من الفيروسات والبرامج الضارة من الوصول إلى الكمبيوتر عبر الشبكات المحلية أو الانترنت، حيث تعمل على تحليل كل المعلومات الواردة من الشبكات ثم تقوم إما بمنعها أو السماح لها بالوصول إلى وحدة البيانات المحمية، كما تقوم أيضا بمنع أجهزة الكمبيوتر من إرسال البرامج الضارة إلى أجهزة أخرى كما هو مبين في الشكل التالي.



شكل (20) يبين طريقة عمل جدار الحماية

(1) الإحالات في النسخة المطبوعة.

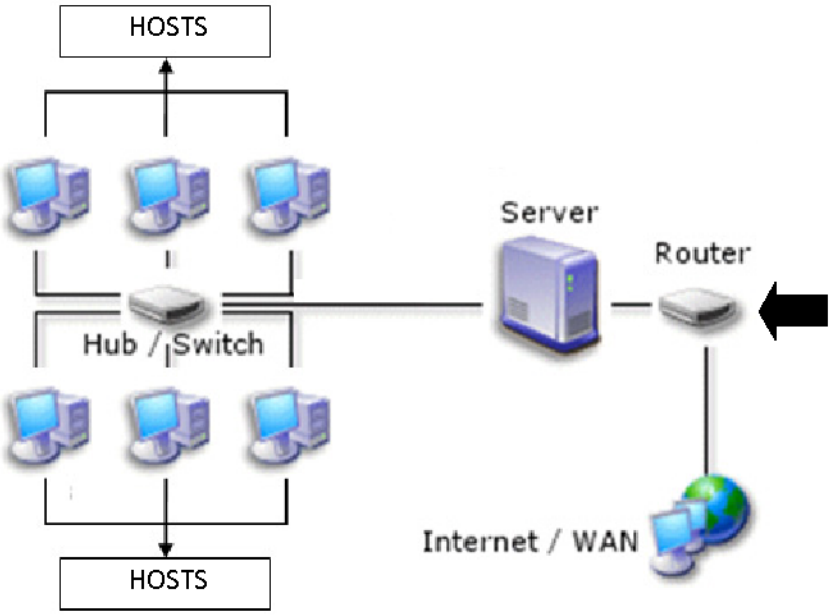
(2) الإحالات في النسخة المطبوعة.

...../...

إضافة إلى ذلك فقد عرفت جدران الحماية أجيالا متنوعة تطورت مع الحاجة الماسة إلى سياسة أمنية رادعة لتحديات جرائم المعلومات، وهي تختلف عن بعضها في الخيارات وفي مجالات الاستخدام؛ فمنها ما يستخدم سياسات أمنية أكثر بساطة، ومنها ما يتيح إمكانية اختيار العديد من السياسات الأمنية وذلك وفق طبيعة الأخطار أو التهديدات التي يجب مواجهتها، ومن أبرز أنواع جدران الحماية استعمالا؛ الموجه الحاجب Screening Router ، وخادم الوكيل ــ الوسيط ــ Proxy، والحارسGuard وبيانها في الفروع التالية[1]:

الفرع الأول ــ الموجه الحاجب Screening Router

هو أبسط أنواع جدران الحماية لكنه يتمتع بفعالية ممتازة، ففي العادة لا تكون الحواسيب المضيفة Hosts موصولة مباشرة بالشبكات الواسعة* WANS لكنها توصل بواسطة موجه Router الذي بدوره يقوم باستقبال حزم الرسائل Packets وبناء على جداول التوجيه المخزنة لديه يقوم بتمرير الحزم الواردة إلى أحد المنافذ العديدة التي تتولى بدورها إيصال كل حزمة إلى وجهتها كما هو مبين في الشكل التالي.



شكل رقم (21): يظهر الجدار الناري الموجه الحاجب Screening Router وهو يصل شبكة محلية بشبكات واسعة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وللموجه الحاجب إمكانية العمل في كلا الاتجاهين بحيث يقوم بتمرير حزم البيانات الآتية من الشبكة الداخلية وبثها إلى العالم الخارجي، كما يستقبل الحزم الواردة من الخارج ويمررها إلى العناوين المرسلة إليها في الشبكة الداخلية، وذلك بعد ترشيحها وهي عملية تتم على مستوى الحزمة*، ولأن الموجه يقوم بتمرير الآلاف من الحزم في الثانية الواحدة فإن قواعد الحجب أو السماح لابد أن تكون بسيطة ليستطيع الموجه أن يختبرها ويطبقها بسرعة فائقة دون أن تتأثر حركة مرور البيانات، ويتم ذلك عن طريق فحص الموجه للمعلومات الموجودة في مقدمة الحزمة فقط Header وليس كل محتوياتها.

وحسب البروتوكول المستخدم فإن المقدمة عادة تحتوي على كل من "عنوان المصدر"، و"عنوان الوجهة"، و"البروتوكول المستخدم"، و"مَنفذ الإرسال"، و "منفذ الوصول"، وعدد حروف الحزمة، وترتيب الحزمة داخل الرسالة، والأولوية، إضافة إلى بعض المعلومات الأخرى التي يتم تضمينها خصيصا لاكتشاف أخطاء الإرسال بحيث يستطيع من خلالها الموجه اكتشاف ما إذا كانت الحزمة الآتية من الخارج تدعي أنها صادرة من الداخل أم لا، وذلك عن طريق التحقق من أن عنوان المصدر ليس أحد عناوين المصدر للحواسيب المضيفة الداخلية. كما يسمح الموجه ببرمجته عبر اختيارات متاحة من بينها تمرير الحزم من الداخل إلى الخارج فقط، أو من الخارج إلى الداخل فقط[1].

الفرع الثاني ــ خادم الوكيل Proxy :

خادم الوكيل برنامج يعالج حركة النقل إلى الأنظمة المضيفة الخارجية نيابة عن البرامج المستضافة المشتغلة على شبكة محلية، حيث يمكن للمستخدمين الوصول إلى الانترنت عبر جدار ناري والإبحار في العالم الخارجي لكن الدخلاء لا يمكنهم دخول الشبكة المحلية، كما يتوسط هذا الخادم بين مستخدم الشبكة الداخلية وبين خادم آخر على الإنترنت وبذلك فإن البروكسي قد يكون مستضافا وخادما على حد سواء، وهي إحدى الفوائد الرئيسية لاستعمال خادم الوكيل.

---

(1) الإحالات في النسخه المطبوعه.

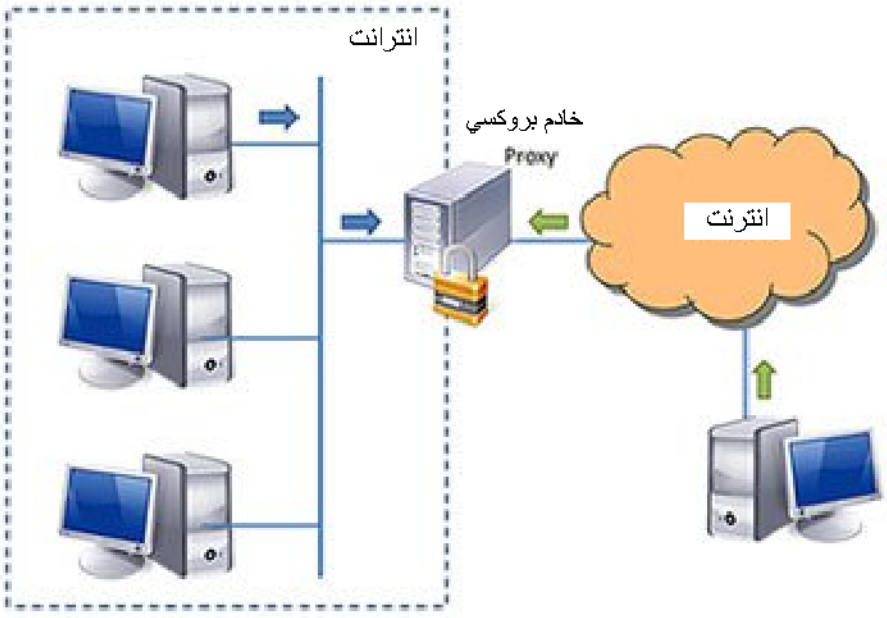
(2) الإحالات في النسخة المطبوعة.

...../...

وفي العادة يكون جدار الحماية "Proxy" عبارة عن جهازا مستقلا، بحيث يتم تحديد إمكانياته ولا يتيح للمستخدمين إمكانية التحكم فيه كإجرائهم لأي تعديل على القواعد المبرمجة داخله، وهو تضييق يمنع فتح أي ثغرات محتملة يمكن الاختراق من خلالها.

ومن مهام الخادم الوكيل التعرف على شخصية المتصل كالاسم، وكلمة المرور، وأي معلومات أخرى للتأكد من شخصيته، وبعد ذلك يمرر المعلومة للحاسوب المطلوب الاتصال به فقط وفق ما تحصل عليه من معلومات سليمة.

ومن ميزاته؛ أنه يحمي خدمات موقع الويب أو الشبكة الداخلية "الانترانت" غير الحصينة، كما يقوم بإخفاء العنوان الإلكتروني IP للمستخدم عند استعمال الانترنت وهي طريقة تجنب لفت انتباه الدخلاء غير المرغوب فيهم مما يزيد من أمان النظام[1].



شكل رقم:(22) يبين تحكم الوسيط Proxy في أمن المعلومات عبر الشبكة الداخلية و شبكة الانترنت

الفرع الثالث ــ الحارس Guard :

هو جدار ناري يشبه الخادم الوكيل Proxy من حيث برمجته لكنه يتميز بدرجة عالية من التعقيد؛ فهو يتلقى وحدات بيانات البروتوكول ويحللها ثم يقرر مدى السماح للمعلومات بالمرور من عدمها، كما يسمح أيضا بتمرير وحدات معلوماتية أخرى بديلة للحصول على نتائج إضافية، كما

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../.....

يقرر آليا الخدمات التي يجب أن يؤديها نيابة عن المستفيد وذلك اعتمادا على المعلومات المتاحة ومثال ذلك: كأن تتيح بعض المكاتب الافتراضية لمرتاديها إمكانية الاستفادة من الاطلاع المجاني على ملخصات البحوث والوثائق، بحيث تفرض رسوما معينة في حال رغبة المستخدم الحصول على الوثيقة كاملة وذلك لدفع حقوق الملكية الفكرية، فإذا ما تم ذلك يحصل المستخدم بطريقة آلية على مراده.

وتعتبر السياسة الأمنية للمعلومات التي يطبقها الجدار الناري "الحارس" أكثر تعقيدا وهو ما يجعله أكثر عرضة للخطأ مقارنة بالجدران النارية الأخرى وهي أحد عيوب الحارس[1].

المطلب الثالث: تشفير البيانات DATA Encryption :

الفرع الأول: مفهوم التشفير وأهدافه.

يعرّف التشفير على أنه علم التقنيات الرياضية المتعلقة بعدد من مظاهر أمن المعلومات كالوثوقية (Confidentiality) وتكامل البيانات (Data Integrity) وإثبات شخصية الكينونة (Entity Authentication) وإثبات شخصية مصدر البيانات (Authentication Data Origin)، والتشفير ليس فقط وسيلة لتزويد أمنية المعلومات وإنما عبارة عن مجموعة من التقنيات.[2]

فالتشفير هو إجراء أمني يحافظ على سرية المعلومات، وذلك بعمله على تحويل وترجمة المعلومات المقروءة إلى رموز مبهمة، حيث إذا تم الوصول إليها من قبل أشخاص غير مخول لهم الإطلاع عليها فإنهم لا يتمكنون من فهمها بسبب تحولها إلى خليط من الرموز والأرقام والحروف الغير مفهومة، فعملية التشفير تنطوي على تحويل النصوص المقروءة إلى نصوص مشفرة ويستخدم في هذا التقنية ما يسمى بمفاتيح تشفير الرسالة encryption وفك تشفيرها decryption وهي مفاتيح تستند إلى صيغ رياضية (خوارزميات) معقدة، وتعتمد قوة وفعالية التشفير على عاملين أساسيين؛ الخوارزمية، ودرجة سرية المفتاح المستعمل في فك التشفير[3]، وكل ذلك من أجل تحقيق جملة من الأهداف الأمنية التي من بينها التغلب على الأخطار الآتية:

- منع الإطلاع على المعلومات المحظورة .

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

- منع كل محاولات تعديل البيانات المنقولة عن طريق الشبكة .
- منع محاولات إعادة توجيه البيانات إلى وجهه أخرى .
- منع كل العمليات التي من شأنها أن تأخر إيصال بعض الرسائل أو تغيير محتوياتها .
- منع إقحام رسائل زائفة ضمن الرسائل المنقولة عبر الخط .
- التصدي لانتحال شخصية المستخدم الحقيقي وتغيير كلمات السر الخاصة بالمستفيدين.
- منع كل تعديل في البيانات المخزنة على الحواسيب نفسها .

الفرع الثاني: آليات تشفير البيانات.

تحتاج عملية تشفير البيانات وفكها إلى ثلاثة عناصر مجتمعة وهي: رقم الأساس، والمفتاح العام، والمفتاح الخاص.

فرقم الأساس يتم إصداره إما عن طريق برنامج مخصص لهذا الغرض أو هيئة مستقلة متخصصة في إصداره، ويعرف أيضا برقم التوثيق CA (Certificate Authority) حيث يكون لكل مستخدم رقم أساس مستقل يتم تقسيمه إلى مجموعتين: الأولى تسمى بالمفتاح العام، والثانية المفتاح الخاص، ويكون ناتج ضرب المفتاح العام في المفتاح الخاص يساوي رقم الأساس وهو رقم ضروري لإعادة المعلومات إلى وضعها قبل التشفير، كما يتمتع هذا الرقم بالحماية والتشفير أيضا.

والمفتاح العامPublic Key : هو عبارة عن رقم يتم تداوله بين المستخدمين لتشفير المعلومات أو الرسائل الإلكترونية التي تستوجب الخصوصية، مع العلم أنه لا يتمكن الغير من فك رموز المعلومات المشفرة بهذه الطريقة إلا صاحبها لأنها تحتاج إلى رقم سري يعرف بالمفتاح الخاص، وهو بدوره يسمح بإتمام العملية الحسابية والوصول إلى رقم الأساس، ومن ثم فتح البيانات.

والمفتاح الخاص Private Key : هو مكمل للمفتاح العام لأجل الوصول إلى رقم الأساس وإعادة المعلومات المشفرة لوضعها الطبيعي قبل التشفير، وهو عبارة عن هوية إلكترونية تمكن صاحبها من فك أي معلومة مشفرة مرسلة إليه على أساس رقمه العام، وبذلك لا يستطيع أي أحد فك الرموز وقراءة المعلومات المحمية دون اكتمال الحلقة التي لا تتم إلا بمعرفة القيمة الصحيحة للمفتاح العام والمفتاح الخاص.[1]

(1) الإحالات في النسخة المطبوعة.

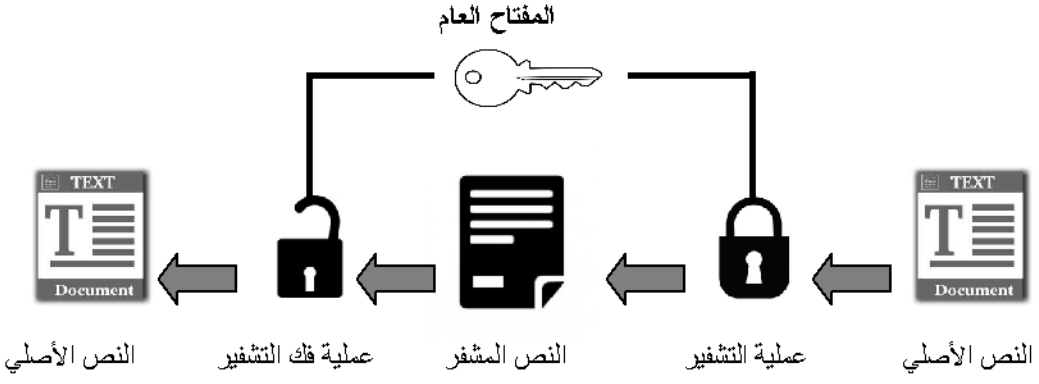
(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثالث: أنواع التشفير.

بناء على المفاتيح المستخدمة في التشفير فإنه ينقسم إلى نوعين أساسيين هما؛ التشفير المتماثل Symmetric Cryptography والتشفير غير المتماثل Asymmetric Cryptography ، حيث يفرق بينهما في مستوى درجة الأمن الذي يحققه كل منهما.

أولا ــ التشفير المتماثل: يستخدم في التشفير المتماثِل كل من المرسل والمستقبِل مفتاحا سريا ذاته (Key Secret) يستعمل في تشفير الرسالة أوفك تشفيرها. حيث يتم الاتفاق بين الطرفين على عبارة المرور (pass phrase) التي سيتم استخدامها، وهي تحتوي على حروف كبيرة وصغيرة ــ باللغة الأجنبية ــ ورموز أخرى، وبعد ذلك تقوم برمجيات التشفير بتحويل عبارة المرور إلى عدد ثنائي ــ لغة الحاسوب ــ ويتم إضافة رموز أخرى لزيادة طولها، حيث يشكِّل العدد الثنائي الناتج مفتاح تشفير الرسالة. وبعد استقبال الرسالة المُشفَّرة، يستخدم المستقبِل عبارةَ المرور نفسها من أجل فك رموز النص المُشفَّر (cipher text or encrypted text)، إذ تترجِم البرمجيات مرة أخرى عبارة المرور لتشكيل المفتاح الثنائي (binary key) الذي يتولى إعادة تحويل النص المُشفَّر إلى شكله الأصلي المقروء، لكن يعاب على هذا النوع من التشفير أن المفتاح السري يتم تبادله دون أمان مما أدى إلى التراجُع في استخدامه.



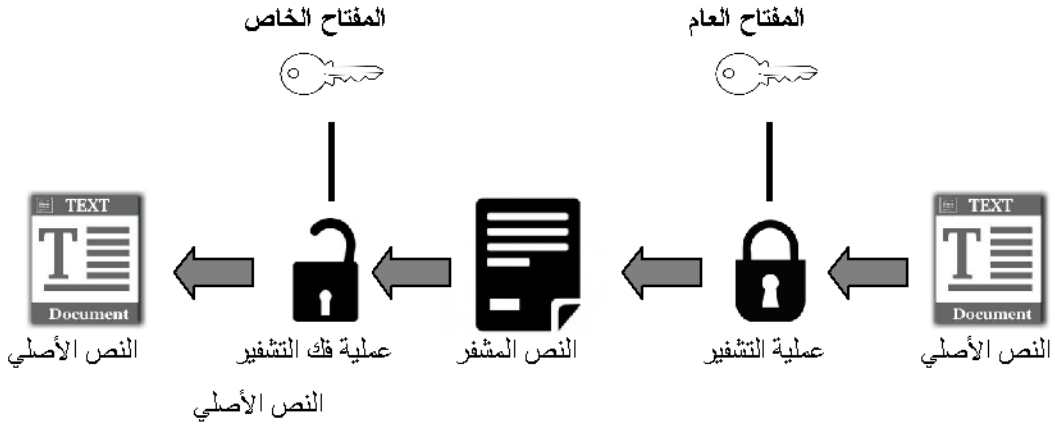
شكل رقم (23): يوضح آلية التشفير المتماثل (Symmetric Cryptography)

ثانيا ــ التشفير غير المتماثل (Asymmetric Cryptography) :

جاء هذا النوع من التشفير كحلاً لمشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل، فعوضاً عن استخدام مفتاح واحد فإن التشفير غير المتماثِل يستخدم فيه مفتاحين اثنين ويُدعى هذان

(1) الإحالات في النسخة المطبوعة.
(2) الإحالات في النسخة المطبوعة.
...../.....

المفتاحان بالمفتاح العام (public key)، والمفتاح الخاص (private key) الذي يحتفظ بسريته لدى جهة واحدة فقط وهو المرسل، وهو يُستخدم لتشفير الرسالة وفكها، أما المفتاح العام فيكون معروفاً لدى أكثر من شخص أو جهة وباستطاعته فك الرسالة التي شفَّرها المفتاح الخاص، كما يمكن استخدامه أيضاً لتشفير رسائل مالك المفتاح الخاص، ولكن لا يمكن لأحد أن يستخدم المفتاح العام لفك رسالة شفَّرها هذا المفتاح العام، إذ أن مالك المفتاح الخاص هو الوحيد الذي يستطيع فك الرسائل التي شفرها المفتاح العام[1].



شكل (24): يوضح آلية التشفير غير المتماثل (**Asymmetric Cryptography**)

المطلب الرابع: التوقيع الإلكتروني

نظرا لما تثيره مشكلة الأمن والخصوصية على الإنترنت من انعدام الثقة بالشبكة واستخدامها في المعاملات التجارية، فإنه تم ابتكار تقنية التوقيع الإلكتروني لرفع مستوى الأمن والخصوصية في تعاملات الشبكة، وهي تقنية تعمل على حفظ سرية المعلومات والرسائل وتمنع أي دخيل من الإطلاع أو تعديل أو تحريف الرسالة، كما يمكنها أن تحدد شخصية وهوية المرسل والمستقبل إلكترونيا للتأكد من مصداقية الشخص وهو ما يسمح بكشف أي تحايل أو تلاعب.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة

...../.....

الفرع الأول: مفهوم التوقيع الإلكتروني

التوقيع الإلكتروني هو عبارة عن شهادة رقمية تصدر عن إحدى الهيئات المتخصصة المستقلة المعترف بها من طرف الحكومة كمكاتب التوثيق القانونية، وتحتوي هذه الشهادة على اسم ومعلومات الرقم المسلسل وتاريخ انتهاء الشهادة ومصدرها [1].

ولقد عرف التوقيع الإلكتروني تعريفات عديدة وذلك باعتبار النظر إليها من الناحية الآلية بمعنى كيف يتم، أو باعتبار النظر إليها من الناحية الوظيفية بمعنى ما هي وظيفته، ومن بين هذه التعريفات ما يلي:

التوقيع الإلكتروني هو: "كل إشارات أو رموز أو أحرف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطة ارتباطا وثيقا بالتصرف القانوني، تسمح بتمييز شخص صاحبها وتحديد هويته، وتنم دون غموض عن رضاه بهذا التصرف القانوني" [2].

وهو: "إجراء معين يقوم به الشخص المراد توقيعه على المحرر سواء كان هذا الإجراء على شكل رقم أو إشارة إلكترونية معينة أو مشفرة خاصة، بحيث يُحتفظ بالرقم أو الشفرة في مكان آمن وسري يمنع استعماله من قبل الغير ويعطي الثقة بأنه صدر من صحابه حامل الرقم أو الشفرة"[3].

كما يعرّف بأنه: "التوقيع الناتج عن إتباع إجراءات محددة تؤدي في النهاية إلى نتيجة معينة معروفة مقدما فيكون مجموع هذه الإجراءات هو البديل للتوقيع التقليدي"[4].

ويعرّف أيضا بأنه: " استخدام معادلات خوارزمية متناسقة يتم معالجتها من خلال الحاسب الآلي تنتج شكلا معينا يدل على شخصية صاحب التوقيع" [5].

وقد عرّفه قانون الأونيسترال النموذجي UNCITRAL [6] بأنه: " بيانات في شكل إلكتروني،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

مدرجة في رسالة بيانات، أو مضافة إليها، أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقّع على المعلومات الواردة في رسالة البيانات".[1]

والملاحظ من هذه التعريفات أنها تدور حول معاني متقاربة وإن اختلفت الألفاظ فأغلبها يشير على أن التوقيع الإلكتروني إجراء أو مجموعة إجراءات تأخذ عدة أشكال سواء رقم أو إشارة أو حرف أو غيرها، كما تسمح هذه الإجراءات بتمييز هوية صاحبها والتعبير عن رضاه.

الفرع الثاني: الفرق بين التوقيع التقليدي والإلكتروني

يتفق كل من التوقيع التقليدي والإلكتروني في كونهما وسيلة هامة يعتد بها في إثبات الهوية والتعبير عن الإرادة، كما يعتمد عليهما في إثبات التصرفات الشرعية والقانونية، إلا أنهما يختلفان في الجوانب التالية:

ـــ يقتصر التوقيع التقليدي في أغلب التشريعات على الإمضاء، وبصمة الخاتم، وبصمة الإصبع، بينما التوقيع الإلكتروني قد يتخذ أشكالا مختلفة وذلك في هيئة حروف، أو أرقام، أو رموز، أو أصوات، أو إشارات، أو غيره من الوسائل التي يكون لها طابع منفرد يسمح بتحديد هوية الأشخاص.

ـــ يتم التوقيع التقليدي في الغالب على دعامة ورقية يوقع في نهايتها، أما التوقيع الإلكتروني فإنه يتم على وسيط إلكتروني من خلال أجهزة الحاسب الآلي أو عبر شبكة الانترنت.

ـــ إذا تم التوقيع الإلكتروني وفق الشروط التشريعية المعمول بها فإنه يصبح دليلا أقوى في الإثبات من التوقيع التقليدي نظرا لسهولة تزوير هذا الأخير.

ـــ كما يتميز التوقيع الإلكتروني عن التقليدي بأنه يؤمّن المستند الإلكتروني من التعديل سواء بالتغيير أو الإضافة أو الحذف، وذلك عن طريق الربط بين المستند وبين التوقيع الإلكتروني.

ـــ بالإمكان فصل التوقيع التقليدي عن المستند سواء بطرق تقليدية أو بطرقة حديثة، بينما التوقيع الإلكتروني لا يمكن فصله عن المستند الإلكتروني بأي حال من الأحوال.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ يمنح التوقيع الإلكتروني للمستند صفة المحرر الأصلي، وبالتالي يجعل منه دليلا معدا مسبقا للإثبات قبل أن يثور النزاع بين الأطراف.[1]

ـــ في حال النزاع، يتطلب التحقق من صحة التوقيع التقليدي العديد من الإجراءات التي يقوم بها خبراء متخصصين ، أما صحة التوقيع الإلكتروني فيتم آليا أثناء عملية التوقيع ذاتها وعند مستقبل الرسالة الموقع إلكترونيا.

ـــ يسمح التوقيع الإلكتروني بإبرام الصفقات وإجراءات التصرفات القانونية عن بعد، دون حضور المتعاقدين في مجلس واحد، كما لا يفقد أي شيء من قوة دلالته على هوية ورضا صاحبه وحجيته القانونية، وهو ما لا يصلح في التوقيع التقليدي.

ـــ في حال التوقيع التقليدي يتمتع الشخص بالحرية الكاملة في أن يعتمد على الإمضاء لإقرار المحررات وله أن يستبدله بالبصمة أو الختم، كما يمكنه أن يجمع بين أكثر من صورة من صور التوقيع التقليدي بدون إذن أو ترخيص من الغير، أما بالنسبة للتوقيع الإلكتروني فإنه يتطلب استخدام تقنية آمنة ودقيقة في إجرائه مما يستوجب تدخل طرف ثالث يضمن توثيق التوقيع الإلكتروني، كما يقوم عند الحاجة بتحديد هوية صاحبه، إضافة إلى أنه يتطلب الحصول على ترخيص من الجهة المخولة بذلك.

ـــ ومن الناحية الشكلية فإن التوقيع التقليدي يعتبر فن وليس علما لأنه عبارة عن رسم يقوم به الممضي وبذلك يسهل تزويره أو تقليده، أما التوقيع الإلكتروني فهو علم وليس فنا، ويصعب تزويره إذا تم استخدامه وفق الشروط الأمنية المعمول بها.

الفرع الثالث: صور التوقيع الإلكتروني

يتخذ التوقيع الإلكتروني صورا وأشكالا عديدة بحسب الطريقة التي يتم بها، والإجراءات المتبعة في إصدار كل شكل منه، وبحسب التقنيات المستخدمة، ومن أهمها ما يلي:

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

1 ــ التوقيع البيومتري (Biometrics)

هو توقيع يعتمد على التحقق من شخصية المتعامل بالاعتماد على الخواص الفيزيائية الطبيعية* للأفراد[1]، وهي صورة علمية حديثة تدخل ضمن تكنولوجيا البصمات والخواص الحيوية والطبيعية.[2]

والتوقيع البيومتري يقوم على حقيقة علمية بأن لكل إنسان صفاته الجسدية الخاصة به، والتي تتميز بالثبات النسبي الذي يجعل لها قدرا كبيرا من الحجية في التوثيق والإثبات.[3]

ومن أنواع التوقيع البيومتري المعمول بها ما يلي:

ــ بصمة الأصابع (Finger Prints).

ــ بصمة العين؛ بصمة شبكية وقزحية العين (Retinal and Iris Scanning).

ــ بصمة معالم الوجه (Facial Recognition) .

ــ خواص اليد البشرية (Hand Geometry) .

ــ بصمة الصوت (Voice Recognition) .

2 ــ التوقيع بالرقم السري:

هي أحد صور التوقيع الإلكتروني التي تعتمد على إدخال رقم سري يتألف من أرقام أو حروف، ويعرف هذا النوع من التوقيع اختصارا بـــ (P.I.N)**. فعند إدخاله يتم آليا مطابقة هذا الرقم برقم سري مخزن سلفا في ذاكرة الحاسوب لمقدم الخدمة المعلوماتية، أو في النظام البنكي الإلكتروني، وفي حال تطابق الرقمان يخول لصاحبه الدخول إلى الموقع الإلكتروني، أو النظام المصرفي الإلكتروني. ويتم تشفير الرقم السري باستخدام تقنية معينة يتم إنشاؤها في المتصفحات على شبكة الإنترنت أو في النظام المصرفي نفسه، وغالبا ما يرتبط هذا التوقيع الإلكتروني بالبطاقات البنكية البلاستيكية الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بشريحة إلكترونية.[4]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

3 ــ التوقيع الرقمـــي:

هي الصورة الأكثر شيوعا على الإطلاق حتى أن البعض يعتقد أنه لا يوجد أي صورة من صور التوقيع الإلكتروني سواها نظرا لما يتحقق فيها من أمان وثقة ولارتباطها بالتعاملات والصفقات التي تتم عبر شبكة الانترنت. كما يعد التوقيع الرقمي من أدق صور التوقيع الإلكتروني والأكثر شيوعا في التعاملات التجارية الإلكترونية لكون تقنيته تجمع بين مهمتي تحديد هوية الموقع وتشفير البيانات وضمان سلامتها من التعديل والتدخل[1].

ويقوم التوقيع الرقمي على أساس تقنية التشفير التي تتطلب استعمال المفتاح العام والخاص الذي سبق التطرق إليه في مطلب تشفير البيانات، ولبيان آلية التوقيع الرقمي نورد المثال التالي:

(وجه المسئول الأول رسالة إلكترونية إلى المدير التنفيذي مفادها تغيير الأرقام المفتاحية لخزنة المال).

أولا ــ لإجراء هذه المراسلة وفق التوقيع الرقمي يتعين التقيد بالخطوات التالية:

الخطوة الأولى: كتابة الرسالة بوسيط إلكتروني كالبريد الإلكتروني مثلا ونصها كما يلي:

السيد المدير التنفيذي،

السلام عليكم ورحمة الله وبركاته،

وفقا للإجراءات الأمنية الدورية المتعلقة بتأمين خزنة المال
نعلمكم بالأرقام المفتاحية الجديدة التي يبدأ سريانها عند
قراءتكم للرسالة وهي كالتالي: **563987142399001**

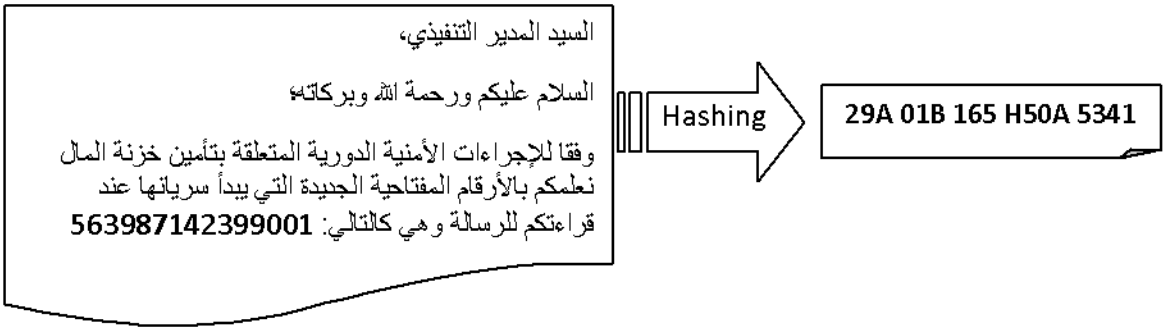
الخطوة الثانية: إجراء مختصر حسابي لهذه الرسالة عن طريق برنامج خاص يقوم بتحويل الرسالة إلى صورة حسابية تعبر عن الرسالة الأصلية حيث يتم تعتيم بيانات الرسالة الأصلية في شكل حسابي، وهي طريقة تعرف بـــ الهاش Hashing ويتم من خلالها تحويل الرسالة الطويلة إلى شفرة نصية قصيرة لينتج لدينا بصمة للرسالة الأصلية وتسمى ((Message digest ، فتصبح كما في الشكل التالي (من اليسار إلى اليمين):

---

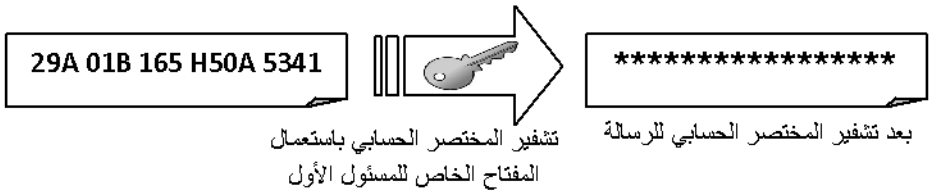
(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

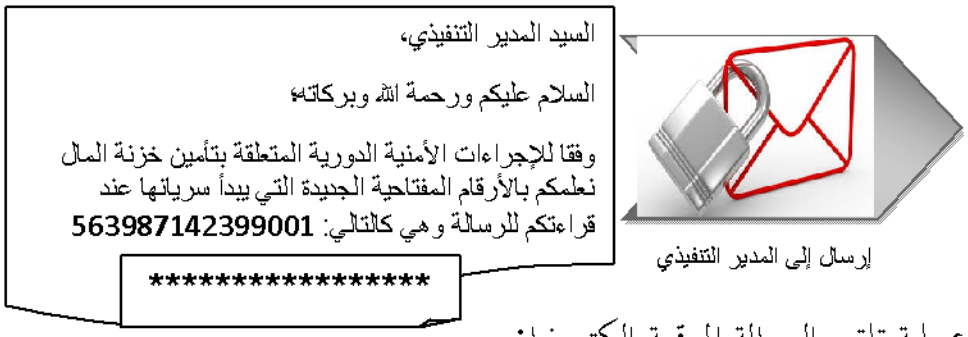
...../...



الخطوة الثالثة: وهي مرحلة تشفير المختصر الحسابي أيضا باستخدام المفتاح الخاص بالمسئول الأول، فيصبح المختصر الحسابي كما هو مبين في الشكل.

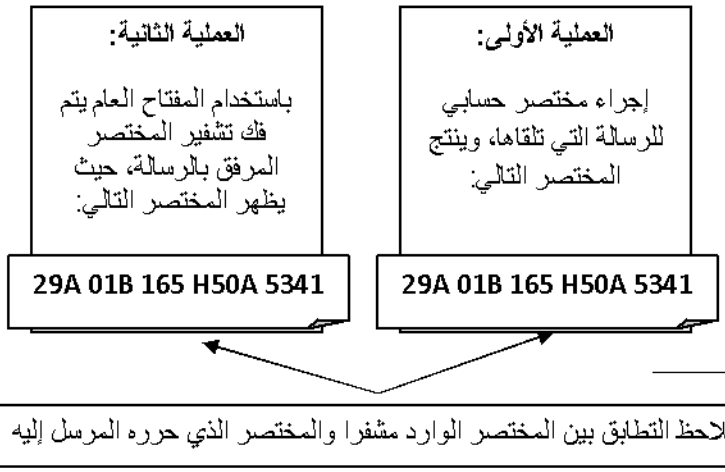


الخطوة الرابعة: ترسل بعد ذلك الرسالة مقرونا معها المختصر الحسابي الذي تم تشفيره كالتالي:



ثانيا: عملية تلقي الرسالة الموقعة إلكترونيا:

يتلقى المدير التنفيذي الرسالة، وحتى يتحقق من صحة نسبتها إلى المسئول الأول وسلامة محتواها من التغيير يقوم بعمليتين:



(1) الإحالات في النسخة المط

(2) الإحالات في النسخة المط

...../.....

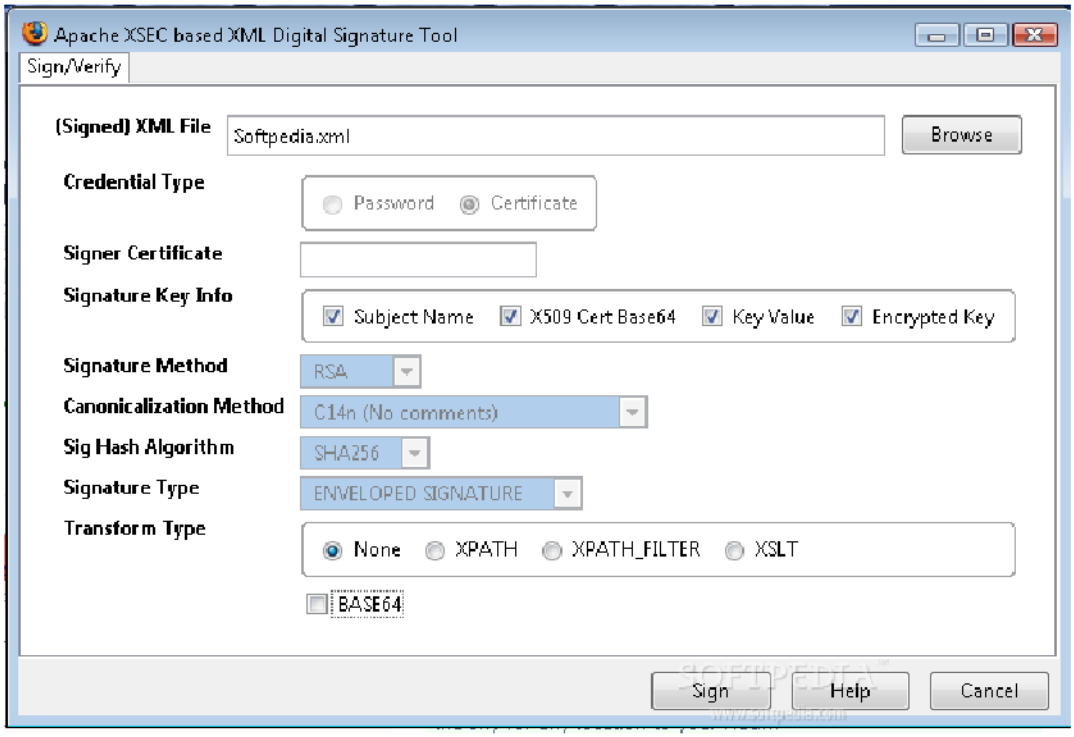
ويترتب على هذه النتيجة ما يلي:

1 ـــ أن المرسل هو بالفعل المسئول الأول.

2 ـــ عدم قدرة المرسل على الإنكار لأن المفتاح الخاص يفترض أن يكون معه دون سواه.

3 ـــ لم يحدث أي تغيير أو تحوير لمحتوى الرسالة، لأنه في حال حصول أي تغير مهما كان متناهي الصغر فمن شأنه أن ينتج عنه مختصر حسابي مختلف تماما عن المختصر الحسابي الأصلي.

مع العلم أن كل هذه العمليات التي تم إيضاحاها تحصل خلال وقت قياسي، ويعود الفضل في ذلك إلى توافر البرامج الخاصة بالتوقيع الإلكتروني والتي تتيح اختيار إجراء التوقيع ضمن مجموعة من الخيارات الموجودة على شريط القوائم أو نافذة الاختيار كما هو مبين في الشكل:



الشكل رقم (25): يبين نافذة اختيارات للتوقيع الإلكتروني

الفرع الرابع: المجالات العملية للتوقيع الإلكتروني.

يقصد بالمجال العملي للتوقيع الإلكتروني كل تصرف أو تعامل عبر الإنترنت يتطلب توقيعا لإثبات هوية صاحب التصرف وبيان توجه إرادته لإقرار التصرف، ومن أهم المجالات العملية للتوقيع الإلكتروني ما يلي:

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

ـــ التجارة الإلكترونية، وتشمل كل معاملة ذات طابع تجاري في مجالات التعامل المختلفة كالبيوع وغيرها من العقود والتصرفات القانونية التجارية الأخرى، والاستيراد والتصدير، وحجز تذاكر السفر، والفنادق، والمعاملات المصرفية بكل أنواعها والتي تتم في شكل محرر إلكتروني يتطلب توقيعا إلكترونيا.

ـــ بطاقات الصرف الآلي بأنواعها، ويقصد بها جميع البطاقات الإلكترونية التي تصدر من البنوك وتمكن أصحابها من السحب النقدي من أجهزة الصرف الآلية كالتي تنتشر في الأماكن العامة، كما تمكن أصحابها من إجراء عمليات الشراء بواسطة أجهزة مخصصة لهذا الغرض وهي متاحة في أماكن البيع، حيث يتم الدفع عن طريق إدخال البطاقة مع كتابة الرقم السري وهو الذي يمثل التوقيع الإلكتروني لصاحب البطاقة.

ـــ الحكومة الإلكترونية، وتشمل المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام ومنها؛ التصاريح المختلفة، والخدمات التي تقدمها الجمارك والضرائب ومصالح الأحوال المدنية، وكذلك ما يرسل للجهات الحكومية من طلبات. [1]

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث: الحاسوب الجنائي ودوره في أمن المعلومات

الحاسوب الجنائي Computer Forensics هو تخصص متفرع من علوم الحاسوب، وهو يعمل على دراسة وتحري الجرائم المعلوماتية باعتباره أحد وسائل الإثبات الرئيسية خلال المحاكمات في الجرائم الإلكترونية، وسواء كانت تلك الجرائم تهدد الأمن القومي أو لها علاقة بإساءة استعمال الحاسوب أو لحل النزاعات المدنية.

والإثبات الجنائي هو نشاط إجرائي موجه مباشرة للوصول إلى اليقين القضائي طبقًا لمعيار الحقيقة الواقعية، وذلك بشأن الاتهام أو أي تأكيد أو نفي آخر يتوقف عليه إجراء قضائي[1]، وعليه فإن وسائل الإثبات هي كل ما يستخدم في إثبات الحقيقة أو ما يفيد في إظهار عناصر الإثبات المختلفة ـــ أي الأدلة ـــ ونقلها إلى المجال الواقعي الملموس [2]، علما أن مسألة الإثبات في نظم الحاسوب والإنترنت تثير صعوبات كبيرة أمام القائمين على التحقيق، ويرجع ذلك إلى جملة من العوائق التي من بينها صعوبة الحصول على الدليل الملموس حيث يشكل تشفير البيانات المخزنة إلكترونيًا أو المنقولة عبر شبكة الانترنت عقبة كبيرة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة ، كما أن سهولة محو الدليل في زمن قصير يعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والانترنت [3].

المطلب الأول: مفهوم الحاسوب الجنائي ومنهجيته

تعود نشأة الحاسوب الجنائي إلى ثورة الحواسيب الشخصية في الثمانينات[4]، وهو مجال يهتم بتحديد وحفظ واسترجاع وتحليل وتوثيق البيانات المعلوماتية التي يشتبه بأنها استخدمت في الجرائم الإلكترونية[5]، ولقد عرف هذا المجال اهتماما كبيرا خاصة في الولايات المتحدة لعدة أسباب منها

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

تداعيات الحادي عشر من سبتمبر 2001م والفضيحة المالية لشركة أنرون[1] Enron الأمريكية التي حصلت في نفس السنة، الأمر الذي أدى إلى توظيف برامج أكاديمية في مجال الحاسوب الجنائي من أجل تخريج كفاءات مؤهلة تقنيا وجنائيا للتحقيق والتحري في جرائم الحاسوب والانترنت عن طريق ابتكار برامج مطورة لهذا الغرض.

الفرع الأول: تعريف الحاسوب الجنائي.

يعرّف الحاسوب الجنائي بأنه علم تطبيقي متفرع من علم الأدلة الجنائية Forensics science وهو يختلف في أهدافه عن تخصص أمن الحواسيب Computer security الذي يهدف إلى حماية نظم الأجهزة والشبكات من الأعمال التخريبية والاختراقات[2]، كما يتفرع من تخصص الحاسوب الجنائي تخصص دقيق مهتم بالشبكات والانترنت يعرف بـــ Network/Internet forensics وهو يهتم بالتحري والتحقيق في جرائم الشبكات[3].

الفرع الثاني: منهجية الحاسوب الجنائي في التحقيق.

إن إجراءات التحقيق في الجرائم الإلكترونية تشبه في عمومها الإجراءات التقليدية كالمعاينة والتفتيش، والمراقبة، والتحريات، والاستجواب، إضافة إلى جمع الأدلة وتحليلها، لكن يجري ذلك في بيئة رقمية تتعامل مع الحواسيب والشبكات ووسائط التخزين ووسائل الاتصال ونحوها، كما يقوم الحاسب الجنائي بدور المحقق معتمدا في ذلك على ستة نماذج لخصها مختصون في علم الحاسوب الجنائي وهي كما يلي:[4]

1 ـــ نموذج لوسنت « Lucent Model » : ويقوم هذا النموذج في التحقيق على الاكتساب Acquire ، والتصديق Authenticate ، والتحليل Analyze.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ــ نموذج KPMG: ويتكون من أربع عناصر هي: التعرف على الدليل الرقمي، والاحتفاظ بالدليل الرقمي، تحليل الدليل الرقمي، وعرض الدليل الرقمي.

3 ــ نموذج Dittrich and Brezinski : وهو نموذج ينسب لـــ Brezinski الذي يعمل في مركز الاستخبارات الأمريكية وDittrich الذي يعمل كخبير أمني في جامعة واشطنطن، ويتكون من ست خطوات هي: إعداد الخطة، وحماية مكان الجريمة، وتوثيق الموجود في مكان الجريمة، والبحث عن أدلة، والاحتفاظ بها ثم معالجتها.

4 ــ نموذج جامعة ييل الأمريكية Yale University : قام بصياغة هذا النموذج Eoghan Casey المشرف الأمني لأنظمة جامعة ييل، ويتكون من ست خطوات؛ الإعدادات القبلية، التخطيط، التمييز، الاحتفاظ والتوثيق والجمع، التصنيف والمقارنة وأخيرا إعادة بناء الجريمة.

5 ــ نموذج ميتر Mitre : اقترح هذا النموذج Gary Palmer من شركة Mitre الأمنية، ويتكون من عنصرين هما: علاقة الأدلة بالجريمة وموثوقية الأدلة المستخلصة.

6 ــ نموذج قسم العدل الأمريكية US Departement of Justice : وهو من محتويات التشريع المعروف في دليل مكتب العدل الأمريكية عن الجرائم الإلكترونية، حيث ذكر الدليل أربع إجراءات تتخذ عند البحث في أجهزة الحاسوب وهي: البحث في جهاز الحاسوب، وطباعة محتوياته أثناء التحري، والبحث في جهاز الحاسوب ونسخ محتويات بعض ملفاته إضافة إلى نسخ محتويات الجهاز في موقع الجريمة وبعدها، وفصل جميع الأجهزة المتصلة بالحاسوب وأخذها لمعمل الحاسوب الجنائي.

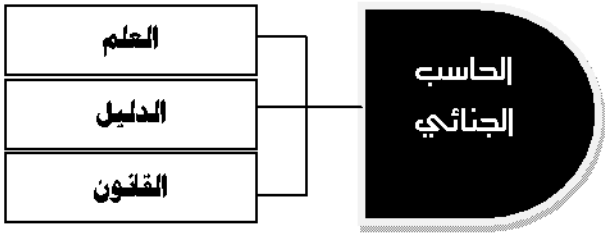
وبناء على ذلك نستنتج أن الحاسب الجنائي يستلزم مجموعة من العناصر هي: العلم بمجال الحاسوب والانترنت، والكفاءة في التحكم في برامج التحقيق والتحري واستخلاص الأدلة، بالإضافة إلى معرفة ما يمكن استخدامه كدليل لدى المصالح القضائية، ثم الإلمام بالخطوات القانونية لتجريم المشتبه به[1] ويمكن تمثيل ذلك بالشكل التالي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...



شكل رقم (26): يبين العناصر المكونة للحاسب الجنائي

المطلب الثاني: برامج الحاسوب الجنائي

تلعب البرامج التطبيقية دورا هاما لمساعدة المحققين في جمع الأدلة في وقت قياسي وهي نوعان: برمجيات خاصة بأمن الحاسوب والشبكات وهو ما سبق التحدث عنه في المبحث السابق، والتي تهدف إلى حماية الحواسيب والشبكات من الاعتداءات حيث تقوم بمراقبة العديد من مجريات الأنشطة والعمليات وتحتفظ بسجلات خاصة بها المعروفة بـــ Logs وهي من بين الأدلة التي يجد فيها فريق التحقيق الكثير من المعلومات المساعدة في إبراز معالم الجريمة.

والنوع الثاني عبارة عن برمجيات مطورة في مجال التحقيق الجنائي الإلكتروني، وهي بمثابة الأدوات المساعدة لفحص الحواسيب والشبكات حيث تمتاز بالدقة والسرعة النسبية في البحث عن الأدلة والآثار الرقمية التي يخلفها الجناة، كما تساعد خبراء التحقيق في جمع كل المعلومات المفيدة بشكل عام، ومن أبرز هذه البرامج ما يلي:

1 ـــ برامج النسخ الاحتياطي الجنائي:

وهي تطبيقات تستخدم لاستنساخ الأقراص الصلبة التي تحتوي عليها الحواسيب محل التحقيق وذلك بهدف إجراء الفحوصات عليها دون تعريض الأقراص الأصلية لأي تغيير، ومن أشهر هذه البرامج التطبيقية برنامج Safeback وبرنامج Encase وبرنامج ProDiscover وبرنامج DD الذي يعمل في بيئة نظام اليونيكس[1].

---

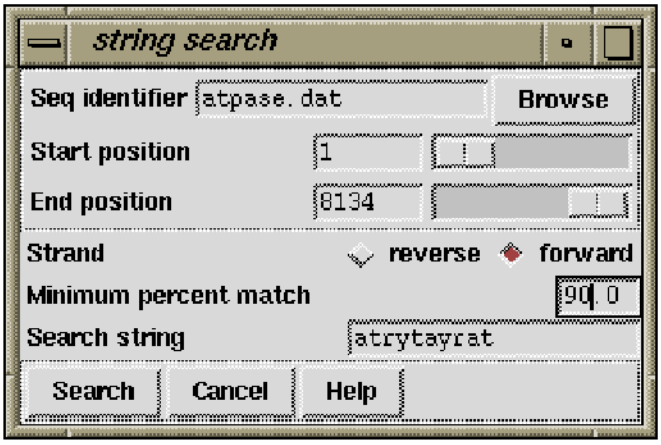
(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ـــ برامج البحث عن المفردات النصية:

وهي تطبيقات تستخدم في البحث عبر البيانات الرقمية عن الملفات التي تحتوي على مفردات مفتاحية عادة ما تكون لها علاقة بالقضية، فيكفي كتابة كلمة أو لفظ معين ويبدأ البرنامج بالبحث عنه واستخراج كل ملف له علاقة بالكلمة وهو ما يوفر على فريق التحقيق الكثير من الوقت والجهد، ومن بين هذه البرامج Et Search وبرنامج String Search وغيرها[1].



شكل رقم (27): يظهر نافذة أوامر برنامج البحث عن المفردات النصية String Search [2]

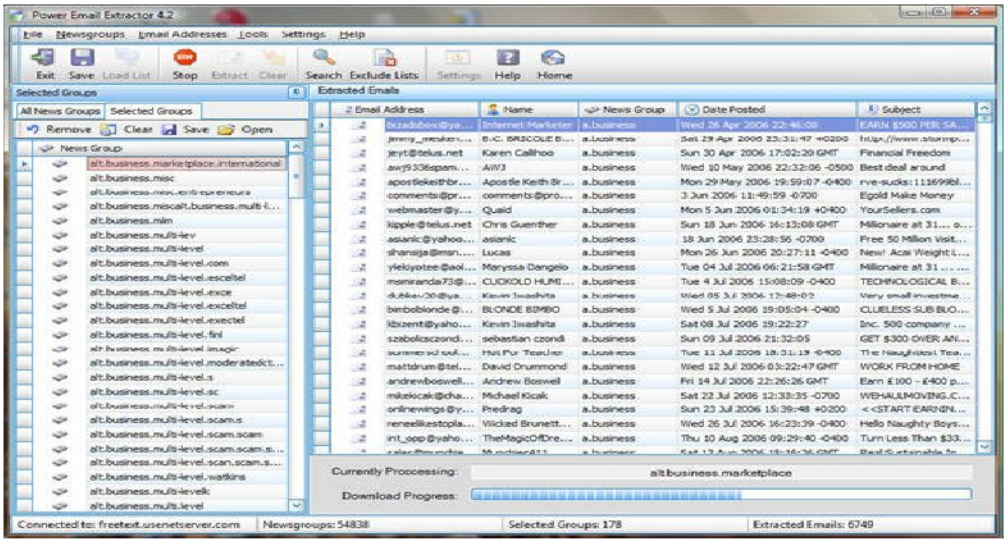
3 ـــ برامج استعادة البيانات المحذوفة:

هناك اعتقاد خاطئ لدى الكثير من مستخدمي الحاسوب بأن حذف أي ملف يعني زواله نهائيا، لكن الحقيقة أن البيانات المحذوفة يتم تخزينها إلكترونيا في جانب معين بالقرص الصلب ولا تزول نهائيا إلا بمرور الوقت، ولذلك يمكن استعادتها مرة أخرى عن طريق برامج تطبيقية مخصصة لهذا الغرض كبرنامج GetFree الذي يعمل بأنظمة النوافذ widows، وبرنامج Extractor الذي يعمل بأنظمة اليونيكس UNIX، وهي برامج جد هامة في مجال التحقيق الإلكتروني [3].

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة

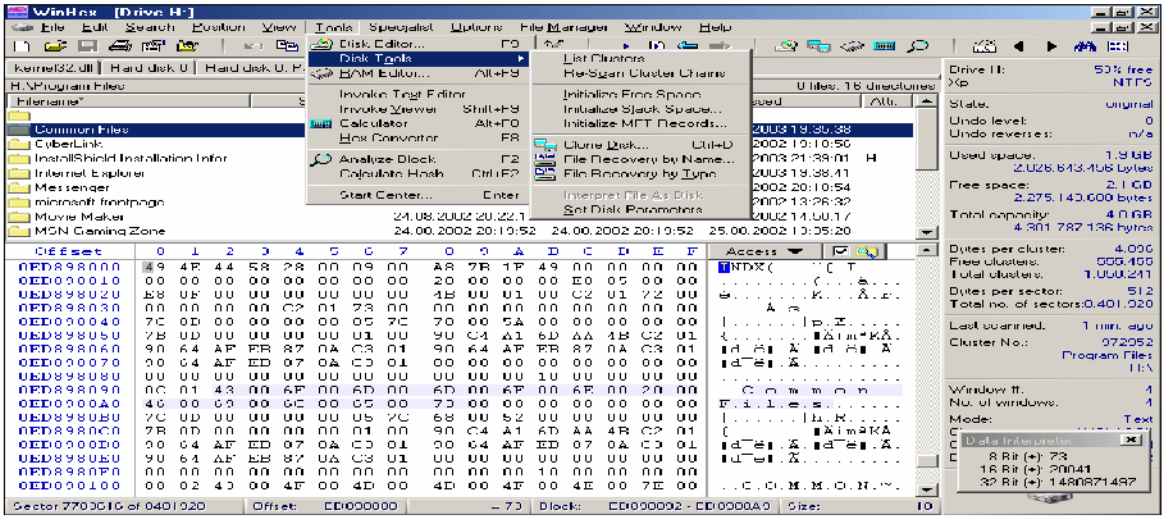
...../...



شكل رقم (28): يظهر نافذة عمل لبرنامج Extractor وهو يعمل على استرجاع الملفات الإلكترونية التي تم محوها من الحاسوب [1]

4 ـــ برامج تحرير الملفات الست عشرية Hexadecimal Editors :

هي برامج تطبيقية ذات أهمية عالية إذ تساعد المحققين في تحليل الملفات والتعرف على طبيعة البيانات التي تحتوي عليها، حيث تقوم هذه البرامج بالتركيز على البناء الثنائي للملف محل التحقيق معتمدة في ذلك على مجموعة من الرموز ذات الدلالة المتواجدة في بداية الملف، ومن خلالها يتمكن خبراء الحاسب الجنائي من تحديد نوع الملف بدقة فيتسنى لهم قراءته وفق التطبيق الأصلي له، ومن أشهر هذه البرامج عامة؛ برنامج Grander وبرنامج WinHex .[2]



شكل رقم (29) يبين نافذة عمل لبرنامج Winhex [3]

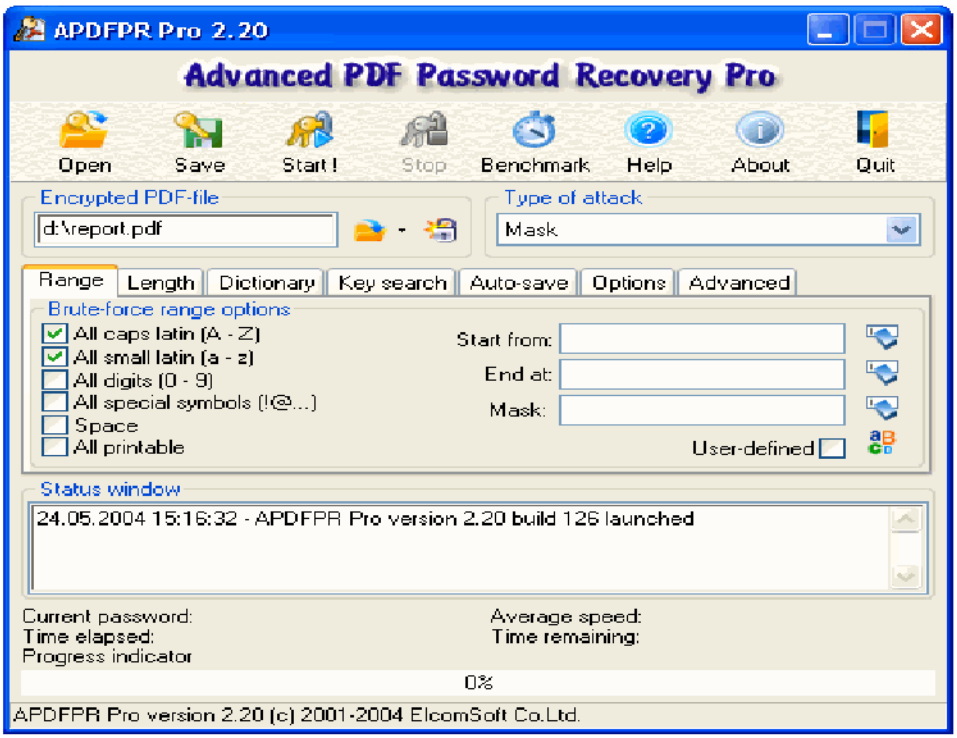
(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

5 ـــ برامج كسر مفاتيح الحماية للملفات:

يصادف فريق التحقيق العديد من الملفات الإلكترونية المحمية بكلمات مرور سرية تمنع أيا كان من الإطلاع على محتوياتها، ولذلك فإنهم يلجئون إلى برامج أنشئت لهذا الغرض حيث تعمل كأدوات كسر مفاتيح الحماية وذلك عن طريق تحليل كلمات المرور وفق احتمالات رقمية جد معقدة وبسرعة متناهية حتى تستخرجها وبذلك يتسنى الاطلاع على الملفات محل التحقيق، ومن بين هذه البرامج التطبيقية على سبيل المثال؛ Password Recovery Suit وبرنامج Office Recovery enterprise وهي تطبيقات تعمل بواسطة برامج مايكروسوفت أوفس Microsoft Office ، وبرنامج Advanced PDF Password recovery Pro للتعامل مع المستندات التي تم إنشاؤها بواسطة برنامج أدوب أكروبات Adobe Acrobat ، وبرنامج Advanced Archive Password Recovery الخاص بالتعامل مع ملفات الأرشفة المضغوطة ذات الصيغ المختلفة مثل Zip، و Rar، و Ace وغيرها[1].



[2] شكل رقم (30) يبين نافذة أوامر لبرنامج Advanced PDF Password recovery Pro

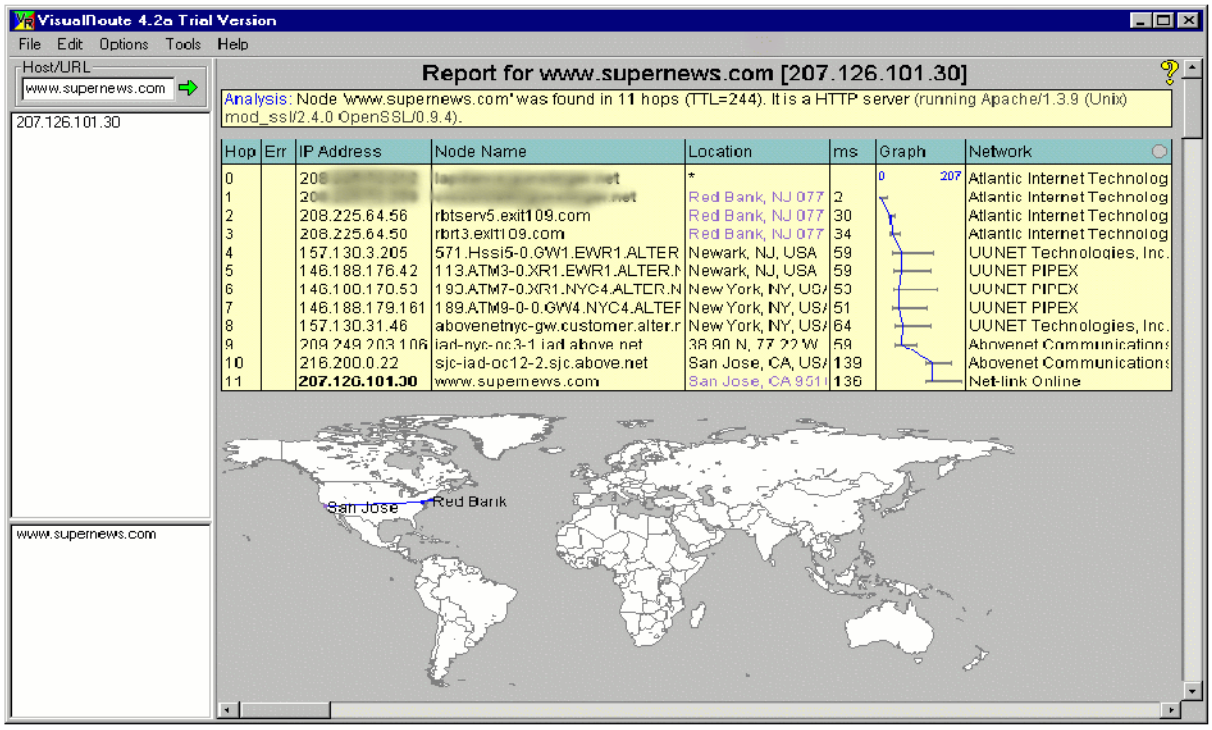
(1) الإحالات في النسخة المطبوعة

(2) الإحالات في النسخة المطبوعة.

...../...

6 ـــ برامج تقفي الاتصال الشبكي:

يستعان بهذه البرامج لمعرفة المصدر الأصلي لأي اتصال شبكي صادر من حاسوب معين سواء عن طريق الشبكة المحلية أو العالمية، وهي عملية تعرف بالتعقب التراجعي Tracing Back حيث تبرز أهمية هذه البرامج على وجه الخصوص عند التعامل مع محاولات الاختراق التي يكون فيها الهاكر متصلا بالنظام المستهدف، ويعرف العديد من هذه البرامج التي يكون بعضها على شكل أدوات ملحقة بأنظمة التشغيل كأداة Traceroute وهي تعمل على أنظمة اليونيكس، وأداة Tracert التي تعمل على أنظمة النوافذ Windows NT/2000/XP، والبعض الآخر يكون على شكل برامج ذات واجهة رسومية كبرنامجي Neotrace Pro و VisualRoute والتي تظهر خط سير الاتصال الشبكي على خارطة العالم وصولا إلى المصدر، وذلك عن طريق تقصي العنوان الشبكي IP Address أو اسم النطاق Domain Name، فتكشف العنوان الشبكي للحاسوب الذي صدر منه الاختراق، إضافة إلى المعلومات المتعلقة بمزود الخدمة الذي تنتمي إليه الشبكة الوارد منها الاتصال، وهي معلومات جد هامة في التحقيق الجنائي[1].



شكل رقم (31): يبين نافذة عمل لبرنامج VisualRoute وهو يقوم بتقفي الأثر [2]

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../.....

7 ــ برامج استعراض الصور:

وهي برامج تقوم بعرض الصور الرقمية على شاشة الحاسوب ويستعملها عامة مستخدمي الحواسيب كما تستغل عند التحقيق في الجرائم الإلكترونية حيث تمكن المحققين من المعاينة الآلية للصور الرقمية والأفلام المخزنة داخل الحواسيب أو على وسائط التخزين الخارجية، وتبرز الحاجة لهذه البرامج في جرائم حيازة ونشر مواد وصور ذات طابع إباحي أو التحريض الإرهابي ونحوه، ومن أشهر هذه البرامج على سبيل المثال؛ ThumsPlus و ACDSee [1].

8 ــ برامج معاينة الصيغ المختلفة للملفات:

يتمثل دور هذه البرامج في تقديم العون لفريق التحقيق من خلال قدرتها الفائقة على تمييز وعرض محتوى الصيغ المختلفة Extensions للملفات المصادرة، ومن أشهر هذه البرامج التطبيقية برنامج Quik View Plus الذي بإمكانه معاينة محتوى 225 صيغة من الملفات المنشئة باستخدام برامج متنوعة. [2]

9 ــ برامج تسجيل وتتبع ضربات لوح المفاتيح:

إن أكثر من يستخدم هذه البرامج هم مجرمو الحواسيب والانترنت وذلك للتجسس على ما يكتبه مستخدم الحاسوب من خلال لوحة مفاتيحه الخاصة بغرض الحصول عل معلومات تفيدهم في الاعتداء على الضحية؛ كاكتشاف كلمات السر لبطاقات الائتمان أو كلمات المرور لدخول نظام حساس وغيره، ومن أمثلة هذه البرامج Revealer Keylogger، و PC Spay Keylogger وBlazingTools Perfect Keylogger، وبالمقابل أيضا فإن الشرطة الإلكترونية تستعمل هذه البرامج وذلك في حالات مراقبة المشتبه به في قضية لها علاقة بجرائم الحاسوب والانترنت وحتى الجرائم التقليدية [3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

الفصل الثاني:
التدابير والتشريعات القانونية لمكافحة الجريمة الألكترونية

المبحث الأول: مفهوم القانون الجنائي وصوره الجزائية

المبحث الثاني: التشريعات القانونية الإقليمية تجاه الجرائم الإلكترونية

المبحث الثالث: التدابير والمعاهدات الدولية لمكافحة الجرائم الإلكترونية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: مفهوم القانون الجنائي وصوره الجزائية

المطلب الأول: مفهوم القانون الجنائي

الفرع الأول: تعريف القانون الجنائي

عرف هذا المصطلح اختلافا في التسمية بين العديد من النظم والباحثين وذلك وفق مبررات معينة، فعرف بقانون العقوبات، كما يعرف عند البعض بالقانون الجنائي، ويعرف أيضا بالقانون الجزائي، ولقد لقيت هذه التسميات انتقادات مختلفة إلا أنها تتفق في كونها قانون يشمل ضمن مواده الأفعال المعتبرة جرائم وعلى ما يقابلها من عقوبات أو تدابير أمنية[1]، ومن تعريفات القانون الجنائي "أنه مجموعة من القواعد القانونية التي تبين الجرائم وما يقرر لها من عقوبات أو تدابير أمن إلى جانب القواعد الأساسية والمبادئ العامة التي تحكم هذه الجرائم والعقوبات والتدابير".[2]

ويقودنا ذلك إلى أن القانون الجنائي يهدف إلى حماية المصالح الجماعية والفردية بأنواعها المادية والمعنوية، كما يسعى إلى توفير الأمن والطمأنينة لأفراد المجتمع، وتحقيق العدالة ونشرها بين الناس كما يهدف أيضا إلى مكافحة الجريمة بأنواعها.

الفرع الثاني: أقسام القانون الجنائي.

ينقسم القانون الجنائي إلى القسم العام و الخاص، ولكل منهما اختصاصه في معالجة موضوع الجريمة و لا يمكن الاستغناء عن أي منهما في تحقيق العدالة، فالقسم العام هو عبارة عن مجموعة قواعد مجردة تحدد أنواع الجرائم بصفة عامة وتقسمها بحسب جسامة عقوباتها إلى جنايات وجنح ومخالفات، كما ترسم الحدود العامة للتجريم[3]. أما القسم الخاص فهو عبارة عن مجموعة القواعد المتصلة بكل جريمة من الجرائم كوحدة قائمة بذاتها[4]، وهو يتضمن القواعد التي تحدد الأركان الخاصة بكل جريمة على حده والجزاءات المقررة لها[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ويعد القسم العام بمثابة تمهيد للصياغة الفنية لنصوص القسم الخاص، لذلك يتضمن القسم العام المبادئ العامة الأساسية تفاديا لتكرارها عند تناول مفردات الجرائم في القسم الخاص، كما يكتسي القسم العام أهميته من جهة الدراسة العلمية حيث أن دراسة القسم العام ترسي المبادئ الأساسية حتى تكون ماثلة في الأذهان عند تناول مفردات الجرائم في القسم الخاص، وعلى هذا النحو لا تستوجب الحاجة إلى تكرار المبادئ العامة عند دراسة جرائم القسم الخاص[1].

كما لا يمكن الاستغناء عن أي من القسمين سواء في فهم القانون أو تطبيقه بحيث يتعذر فهم القسم الخاص إلا عند الرجوع إلى القسم العام لأجل تجريم أفعال معينة كالمحاولة في الجنايات، والشروع في القتل العمدي، والعقاب على المشاركة في الجنايات والجنح[2].

المطلب الثاني: الجزاء الجنائي وصوره

يتمثل الجزاء الجنائي في صورتان أساسيتان هما العقوبة والتدبير الاحترازي، وكل منهما يسعى إلى تحقيق ذات الهدف وإن اختلفت وسائل كل منهما، فما هي العقوبة والتدبير الاحترازي وما العلاقة بينهما.

الفرع الأول: مفهوم العقوبة في القانون الجنائي

أولا ــ تعريف العقوبة في القانون الجنائي:

للعقوبة تعريفات كثيرة في مؤلفات فقهاء القانون الجنائي، ورغم اختلافها في الألفاظ فإنها تتفق في الجوهر إلى حد كبير، حيث تعرّف بأنها: "إيلام مقصود يوقع من أجل الجريمة ويتناسب معها".[3]

وتعرّف أيضا بأنها: " الأثر الذي ينص عليه القانون ليلحق المجرم بسبب ارتكابه للجريمة".[4]

كما تعرّف بأنها " جزاء جنائي يتضمن إيلاما مقصودا يقرره القانون ويوقعه القاضي على كل من ثبت مسؤوليته عن الجريمة".[5]

ويتضح من خلال هذه التعريفات أن جوهر العقوبة هو الألم أو الأذى المنزل على الجاني بسبب ارتكابه الجريمة ويقع عليه كرها عن طريق الهيئة المختصة، وذلك محافظة على المجتمع ومصالحه،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

بالإضافة إلى ردع الجاني من الرجوع إلى الجريمة وإصلاحه.

ثانيا ــ عناصر العقوبة:

بناء على تعريفات العقوبة المطلع عليها أثناء البحث، فإنه يمكن استخلاص عناصرها كما يلي:

1 ــ الإيلام: هو عنصر يلازم كل عقوبة بوصفه جوهرها، ويتمثل الألم في المساس بحق المحكوم عليه سواء في بدنه أو حريته أو ماله، وذلك عن طريق حرمان صاحبه منه كله أو بعضه، كما قد يكون هذا الحرمان مؤقتا أو نهائيا، وقد يقتصر على فرض قيود معينة تحد من استعماله[1].

2 ــ الإكراه: ينطوي الإكراه على معاني القسر والإجبار، فليس من مألوف الأمور أن يتحمل الشخص الإيلام ويرتضي به طوعا، وهي عقوبة منوطة بالسلطة العامة[2].

3 ــ القصد في إيلام العقوبة: فإنزال الإيلام بالجاني هو أثر مقصود يترتب على توقيع العقوبة لتحقيق معنى الجزاء، بينما القبض أو الحبس الاحتياطي كإجراءين من إجراءات التحقيق والمحاكمة لا يعد أي منها عقوبة وإن قيدا حق المتهم في الحرية وسببا له ألما، لأن هذا الألم غير مقصود[3]. ورغم أن الإيلام يرتبط بالعقوبة ارتباطا لازما إلا أنه غير مقصود لذاته وإنما يهدف إلى تحقيق العدالة والردع بنوعيه العام والخاص وصولا إلى هدف العقوبة النهائي وهو مكافحة الجريمة.

4 ــ لزوم الجريمة بالنسبة للعقوبة: فالعقوبة تعد صورة من صور الجزاء الجنائي كمقابل للجريمة التي ارتكبها الجاني، ففور وقوعها ينشأ الحق في توقيع العقاب على المجرم باعتبار جرمه واقعة جنائية منشئة لهذا الأثر القانوني.

5 ــ تناسب العقوبة مع الجريمة: يعد عنصر التناسب أحد المبادئ الأساسية في علم العقاب، فالقيمة الإقناعية للقاعدة الجنائية بما يحقق أهدافها في الردع إنما يعززها تناسب العقوبة التي توقع على الجاني مع الجريمة التي ارتكبها، وقد تفقد هذه القاعدة قوتها الإقناعية إذا كان الألم الملحق بالجاني أقل من المنفعة التي يحتمل أن يجنيها من الجريمة، لأن مبدأ التناسب يقضي مقابلة الشر بشر مثله من أجل تحقيق العدالة.[4]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثالثا ــ خصائص العقوبة الجنائية:

حدد فقهاء القانون الجنائي خصائص العقوبة الجنائية كما يلي:

1 ــ الشرعية الجزائية: ويقصد بها قانونية الجرائم والعقوبات، فالمشرع وحده من يملك الحق في تحديد الأفعال المعاقب عليها والمسماة بالجرائم، كما يحدد الجزاءات التي تقع على مرتكبيها والمسماة بالعقوبات[1]، وهو مبدأ يفرض الفصل بين السلطات الثلاث ــ التشريعية والتنفيذية والقضائية ــ فالسلطة التشريعية هي التي تصنف الأفعال التي تعد جرائم وتقرر الجزاء الجنائي المترتب عليها باعتبارها صاحبة الاختصاص في تشريع القوانين، وهذا ما يعرف بمبدأ "شرعية القاعدة الجنائية" وهو مبدأ ذو قيمة دستورية في معظم الدول حيث يفرد له نصا خاصا في بعض الدساتير الحديثة والقوانين المعاصرة.[2]

وينص مبدأ الشرعية أن "لا جريمة ولا عقوبة إلا بنص قانوني" وهو ما يجعل الاختصاص بالتجريم منحصرا لدى السلطة التشريعية، وبناء على ذلك فإن دور القاضي يتحدد في تطبيق العقوبة التي يقررها النص القانوني ولا يملك الحق في تجريم أي فعل ولو كان يتنافى مع قواعد الدين والأخلاق ــ في القانون الوضعي ــ أو يشكل ضررا على المجتمع ما لم يرد نص في القانون يجرم هذا الفعل ، كما يلزم القاضي بالتقيد بنوع العقوبة ومقدارها وفق حديها الأدنى والأقصى المنصوص عليه، وأن لا يتجاوز ذلك إلا في المواضع التي حددّها القانون[3]، كما يتوجب على محكمة الموضوع أن تقرّر عدم مسؤولية المتهم مما نُسب إليه إذا كان فعله الذي قام به غير معاقب عليه قانونا بنص سابق يجعل من هذا الفعل جريمة[4]. وهي الإشكالية المطروحة تجاه الجرائم الإلكترونية في بداياتها والتي أوقعت المحاكم في أزمة التشريع تجاهها ولا يزال ذلك قائما في العديد من بلدان العالم.

2 ــ شخصية العقوبة: وهي خاصية تفيد عدم إلحاق العقوبة إلا بالشخص المحكوم عليه ولا تطول إلى غيره. فالعقوبة سواء تعلقت بحياة المحكوم عليه كالإعدام إذا كان شخصا طبيعيا، أو الحل إذا كان شخصًا معنويا أو تعلقت بحريته كالحبس مثلا، أو تعلقت بماله كالغرامة والمصادرة فإنه لا

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

يتحملها الغير نيابة عن المحكوم عليه، كما لا ينتقل أثرها المباشر إلى أفراد أسرته، وإن كانت آثارها غير المباشرة تمتد إليهم كفقدانهم لرب الأسرة في حال إعدامه أو سجنه، لكنها تعتبر آثار غير مقصودة ولا يمكن الحيلولة دون تحقيقها.[1]

وهذا ما كرسته الشريعة الإسلامية منذ قرون عديدة، وذلك من خلال نصوص صريحة في القرآن الكريم والسنة النبوية الشريفة كقوله عز وجل: ﴿ وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَىٰ ﴾[2]، وقوله عز من قائل: ﴿ مَّنْ عَمِلَ صَٰلِحًا فَلِنَفْسِهِۦ ۖ وَمَنْ أَسَآءَ فَعَلَيْهَا ۗ ﴾[3]، وورد في الحديث الشريف قوله ﷺ: (لا يؤخذ الرجل بجريرة أبيه ولا بجريرة أخيه)[4].

3 ــ قضائية العقوبة: وتعني هذه الخاصية أن توقيع العقوبة الجنائية من صلاحيات السلطة القضائية، فهي تتمة لشرعية العقوبة، أي أنه كما لا عقوبة إلا بنص فلا عقوبة أيضا إلا بحكم قضائي، ولذلك لا يمكن في القانون الجنائي توقيع العقوبة إلا من محكمة قضائية مختصة وفقا لإجراءات يقررها قانون أصول المحاكمات الجزائية، كما يقتضي تطبيق هذا المبدأ أن ينطق القاضي المختص بالعقوبة المقررة نوعا ومقدارا[5]. وهو إجراء يساهم في المحافظة على حقوق المتهم وحريته بما تتيح له من فرصة المثول أمام القاضي ودفاعه عن نفسه لما يثار ضده من اتهامات وبيان ما أحاط بالجريمة من ظروف وملابسات[6].

4 ــ المساواة في العقوبة: هي خاصية تفيد بأن النص القانوني الذي يتضمن العقوبة يسري في مواجهة كافة الأفراد، بصرف النظر عن اختلاف أجناسهم، أو طوائفهم أو مراكزهم الاجتماعية، كما أن للقاضي مطلق الحرية في تقدير العقوبة المناسبة لكل مجرم على حده بما يتلاءم وظروفه الخاصة، ومدى خطورته، ودرجة مسؤوليته، ولذلك نص المشرع على حدين أدنى وأقصى للعقوبة كي يتمكن القاضي بما له من سلطة تقديرية أن يتخير العقوبة المناسبة[7].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

رابعا ــ أنواع العقوبات:

قسم فقهاء القانون الوضعي العقوبة إلى أنواع عديدة وذلك وفق معايير معينة أهمها:

1 ــ معيار جسامة العقوبة: فمعظم التشريعات الجنائية المعاصرة تقسم العقوبات وفق هذا المعيار إلى جنائية، وجنحية، وتكديرية.

2 ــ معيار الرابطة بين العقوبات: وتقسم العقوبات وفق هذا المعيار إلى عقوبات أصلية وهي المقررة أصلا بمفردها للجريمة باعتبارها من وجهة نظر المشرع الجزائي كافية لتحقيق معنى الجزاء المقابل للجريمة، وعقوبات غير أصلية أو إضافية وهي العقوبات الملحقة بالعقوبة الأصلية، وقد تكون تابعة لها وتسمى بالعقوبة التبعية، كما قد تكون تكميلية كأن تضاف بحكم قضائي إلى عقوبة أخرى لتحقيق الهدف المرجو من الجزاء الجنائي.

3 ــ معيار موضوع العقوبة: وهو معيار يقسم العقوبات إلى عقوبات ماسة بالبدن، وسالبة للحرية ومقيدة لها، وعقوبات مالية وأخرى تمس بالاعتبار، فالعقوبات الماسة بالبدن هي التي تصيب الإنسان في بدنه أو سلامة جسمه كعقوبة الإعدام والجلد والضرب، أما العقوبات السالبة للحرية فهي تسلب حرية المحكوم عليه خلال فترة تنفيذها كالسجن، والعقوبات المالية تصيب المحكوم عليه بذمته المالية كالمصادرة والتغريم.[1]

الفرع الثاني: التدابير الاحترازية

أولا ــ مفهوم التدابير الاحترازية:

تعرّف التدابير الاحترازية بأنها مجموعة من الإجراءات العلاجية التي ينص عليها القانون، ويطبقها القاضي قسرًا على المجرم لمواجهة الخطورة الإجرامية الكامنة في شخصه ودرئها عن المجتمع[2].

وتعتبر التدابير الاحترازية الوسيلة الثانية للسياسة الجنائية في مواجهة الإجرام، فهي تحل محل العقوبة في الحالات التي يتعذر تسليطها على المجرم كما هو الشأن بالنسبة لفاقدي الأهلية الجنائية من

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المجانين والصبية، وفي حالات أخرى تفرض التدابير بجانب العقوبة بغرض إصلاح وتأهيل بعض المجرمين كما في حالة المدمنين على الإجرام والشواذ[1].

ثانيا ــ خصائص التدابير الاحترازية:

تتميز إجراءات التدابير الاحترازية بمجموعة من الخصائص متمثلة فيما يلي:

1 ــ خضوعها لمبدأ الشرعية: فلا يفرض أي تدبير احترازي إلا بنص شرعي، لأن القانون هو الذي يحددها ويبرر تسليطها لمواجهة الخطورة الإجرامية، ويعد مبدأ شرعية التدابير الاحترازية ثمرة لجهود فقهاء الاتحاد الدولي لقانون العقوبات، وذلك حرصا من أن يكون استغلالها على حساب حريات الأفراد[2].

2 ــ خاصية الإجبار: فالتدابير الاحترازية تطبق إجباريا على الجاني نظرا لما تحققه من مصلحة للفرد والمجتمع، خاصة وأن العديد من صورها عبارة عن تدابير علاجية أو إيداع في مؤسسات للرعاية الاجتماعية[3].

3 ــ الصبغة القضائية: مراعاة لحريات الأفراد وصيانتها فإن الجهة القضائية وحدها من تملك الصلاحية في إيقاع التدابير الاحترازية إذا توافرت شروطها على الجاني، حيث يراعي القاضي في ذلك خبرات الأطباء والأخصائيين النفسانيين والاجتماعيين الذين يمدونه بما يحتاجه من معلومات فنية من أجل اتخاذ قرار التدبير[4].

4 ــ عدم التقيد بالزمن: لا يستطيع القاضي مسبقا تحديد متى سيتحقق علاج المحكوم عليه وإصلاحه، باعتبار أن التدبير يواجه حالة مستقبلية لا يمكن التنبؤ بها. ولقد أثارت هذه الخاصية جدلا بين فقهاء القانون حول إمكانية التنسيق والتوفيق بينها وبين مبدأ الشرعية الذي يستلزم تحديد مدة الجزاء[5]، حيث ذهب جانب من الفقه إلى أن عدم تحديد مدة التدبير الاحترازي يشكل تهديدا للحرية الفردية، ولذلك يفضلون أن تحدد السلطة القائمة على التنفيذ الحد الأقصى لمدة التدبير بحسب ظروف المحكوم عليه، وهو ما لجأت إليه بعض التشريعات إلى ربط التدبير بحد أقصى أو بحد أدنى أو بكليهما

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

معا[1].

5 ــ الخاصية الشخصية: فالتدبير الاحترازي هو إجراء يقصد به تفريد الجزاء الجنائي تبعا للشخصية الفردية التي صدرت منها الخطورة الإجرامية، لذلك فإن المنطق يقضي بألاّ تسلط إلا على الشخص الخطر لإزالة خطورته[2].

6 ــ المراجعة المستمرة: وهي من أهم خصائص التدبير الاحترازي، وذلك بجعله يتلاءم مع تطور الحالة ــ نحو الأحسن أو الأسوأ ــ لأنه من الصعب بمكان أن يحدد القانون أو القاضي سلفا مدة التدبير، وبالتالي فإن التدبير المتخذ لا يكون نهائيا إلا إذا ثبتت فاعليته أثناء تطبيقه.

7 ــ التجرد من المسؤولية الأخلاقية: إن فكرة التدبير الاحترازي وجدت أصلا لمواجهة الحالات التي لا يمكن أن تطبق فيها العقوبات، لذا فإن تجرد التدبير الاحترازي من الفحوى الأخلاقي هو ما يميزه عن العقوبة التي تسلط على الجاني نتيجة خطيئته[3]، وهذا باعتبار أن هدف التدبير الاحترازي هو الوقاية وليس العقاب، وهو ما يفسّر إمكانية تطبيق التدبير الاحترازي على عديمي الأهلية والإدراك كالمجنون والصبي بالرغم من تجرد إرادتهما من القيمة القانونية[4].

ثالثا ــ أنواع التدابير الاحترازية:

تعرف أنواع التدابير الاحترازية في التشريعات الجنائية وفق التقسيم الذي يميز بين التدابير الشخصية بنوعيها السالب والمقيّد للحرية والتدابير المانعة للحقوق والتدابير العينية، وبيانها كما يلي:

1 ــ التدابير الاحترازية الشخصية: وتنقسم إلى تدابير شخصية سالبة للحرية، وأخرى مقيّدة لها.

أ ــ التدابير السالبة للحرية: هي مجموعة الإجراءات التي تؤدي إلى سلب حرية المحكوم عليه بهدف علاجه من المرض النفسي أو العقلي أو العصبي الذي دفعه لارتكاب الجريمة أو أفسد سلوكه الاجتماعي، أو بغية إبعاده عن المجتمع أو المحيط الذي يعيش فيه، أو من أجل إقصائه عن الأمكنة التي يخشى بسبب وجوده فيها أن يرتكب هو أو غيره جريمة جديدة[5]، وتتمثل هذه التدابير في أمرين، الأول الحجز في مأوى علاجي كالمصحات المخصصة للأمراض العقلية أو النفسية أو الإدمان على

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المسكرات أو المخدرات بهدف مواجهة حالة الخطورة الإجرامية الكامنة لدى المجرم، ويعد هذا النوع من التدابير سالبا للحرية نظرا لإلزامه للمحكوم عليه بالإقامة في المصحة أو المستشفى العلاجي وإخضاعه للإجراءات العلاجية[1]، والأمر الثاني هو الإيداع في المنشآت المنتجة أو المصنعة، وهو إجراء يحكم به على المجرمين المعتادين والمنحرفين وذوي الميل الإجرامي والمتشردين، وذلك من أجل تعويدهم على العمل بهدف مساعدتهم على الاندماج مع المجتمع، وقد أخذت العديد من التشريعات بهذا النوع من التدبير منها قانون العقوبات الإيطالي[2].

ب ـــ التدابير المقيّدة للحرية: هو إجراء تقيد فيه حريات المجرم جزئيا ومن أهمها:

ـــ الوضع تحت المراقبة: والهدف من ذلك التأكد من مدى صلاح المحكوم عليه عن طريق مراقبة تحركاته، كما يمنع من ظهوره في أماكن لها علاقة بسلوكه الإجرامي خشية عودته إلى الجريمة مرة أخرى[3].

ـــ الإبعاد: في ظل السياسة المعاصرة أصبح هذا النوع من التدابير يقتصر على الأشخاص الأجانب، حيث تلجأ الدولة إلى إبعاد كل أجنبي عن أراضيها إذا تبين أنه يشكل خطرا على السلامة العامة، ولا تسمح له بالعودة مطلقا، أو تسمح له بذلك بعد مرور فترة معينة من الزمن[4].

ـــ حظر ارتياد أماكن معينة: وهو تدبير يمنع فيه القانون بعض الأشخاص من التردد على أماكن معينة كالحانات والملاهي نظرا لما تهيئه هذه الأماكن من ظروف ارتكاب جرائم جديدة، ويهدف هذا التدبير إلى الحيلولة بين الجاني وبين ارتكابه الجريمة[5].

ـــ حظر الإقامة في مكان معين: هو تدبير يحظر على الشخص الخطر إقامته في إقليم أو مكان معين بغرض عزله عن الظروف البيئية التي تسهّل عليه ارتكاب جريمة جديدة، كما قد يخضع المعني لإجراءات إشراف ومساعدة وتفرض عليه واجبات معينة لتسهيل تكيفه مع مجتمعه في مكان إقامته الجديد[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ الرعاية اللاحقة: وهو تدبير يسعى إلى تكملة جهود إعادة التربية والتأهيل التي بذلت أثناء وجود المجرم في المؤسسة العقابية، وتسهر على تنفيذ هذا التدبير مؤسسة معترف بها لدى الدولة حيث توفر للمعني العمل وإسداء النصح والمعونة إضافة إلى مراقبة سلوكه ورفع تقرير عن حالته مرة كل ثلاثة أشهر إلى المحكمة التي قضت بالتدبير، وهو ما نصت عليه العديد من التشريعات الجنائية الوضعية[1].

2 ـــ التدابير الاحترازية المانعة للحقوق: من أهم هذه التدابير؛ التجريد من الولاية أو الوصاية، وحظر مزاولة العمل.

ـــ التجريد من الولاية أو الوصاية: المقصود به حرمان المحكوم عليه من حق التصرف على نفس أو مال من يخضعون لولايته أو وصايته من الصغار، وقد يكون هذا التجريد عاما بحيث يشمل كل من يخضع لولايته ووصايته، كما قد يقتصر على بعضهم دون الآخر[2]. ويعود الغرض من هذا التدبير هو إبعاد القصّر عن مواطن الفساد والخطورة من أجل رعاية شؤونهم ومصالحهم على الوجه الذي تتحقق فيه مصالحهم[3].

ـــ حظر مزاولة العمل: وهو تدبير يحرم بموجبه المعني من مزاولة مهنة أو عمل ما إذا كان سلوكه الإجرامي يمثّل خروجا على أصول أو تقاليد أو واجبات هذا العمل وكان هذا العمل يهيئ فرصة ارتكاب جريمة جديدة، كمنع الطبيب الذي يرتكب جرائم الإجهاض من ممارسة مهنة الطب، أو منع التاجر الغشاش من أعمال التجارة، ومنع الموظف المرتشي من العودة إلى الوظيفة العامة[4].

3 ـــ التدابير الاحترازية العينية: نظرا لرؤية المشرع الوضعي في أن بعض الأشياء قد تشكل عاملا من العوامل التي تسهل على الجاني ارتكاب الجريمة، فقد قرّر تدابير عينية يجرد فيها هذه الأشياء من الشخص المعني بهدف إبعاده عن الإجرام[5]، ومن أمثلة ذلك ما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ المصادرة: ويقصد بها مصادرة الدولة لأموال الجاني قهرا إذا ثبت مصدرها من الجريمة أو استعملت في ارتكابها[1]، وهذا بهدف توقي الخطورة الإجرامية الكامنة في شخص المجرم كأن يستعمل المال ثانية في ارتكاب الجريمة التي حتما ستشكل خطورة على المجتمع[2].

وتطبيقا لمبدأ شخصية العقوبة فقد تكون المصادرة عقوبة إذا وردت على شيء مملوك للمحكوم عليه، كما قد تكون تدبيرا احترازيا إذا وردت على شيء مملوك للمحكوم عليه أو لغيره وحيازته غير مشروعة، حيث تستوجب المصادرة بهدف منعه من استعماله في ارتكاب الجريمة[3].

ـــ الكفالة الاحتياطية: هي عبارة عن إيداع مبلغ من المال أو سندات عمومية أو ربط كفيل ذي ملاءة مالية أو عقد تأمين ضمانا لحسن سير سلوك المحكوم عليه أو تلافيا لجريمة أخرى[4].

وهو تدبير يهدف إلى خلق موانع نفسية لدى المعني لإبعاده عن سلوك طريق الإجرام وتهديده بضياع قيمة الكفالة عليه إذا حاد عن السلوك القويم مما يساهم في تفادي وقوع الجرائم التي قد تصدر عنه[5].

ـــ إقفال المحل: ويقصد به منع المحكوم عليه من ممارسة نفس النشاط الذي صدر بشأنه الحكم، كي لا يستعين بظروف العمل في المحل ويرتكب جرائم أخرى، وهو تدبير الهدف منه مواجهة الخطورة الإجرامية للمحكوم عليه[6].

ـــ توقيف الهيئة المعنوية عن العمل أو حلّها: يتمثل التوقيف في منع الشخص المعنوي من مباشرة نشاطه المعتاد خلال المدة المقررة في الحكم، أما المقصود من حلّ الهيئة المعنوية هو تصفية أموال هذه الهيئة وزوال شخصيتها المعنوية[7]. وهذا التدبير أمر جوازي للمحكمة يرجع تقديره للقاضي، ويقضي به على الهيئات الخاصة دون الحكومية أو المؤسسات الرسمية، كالشركات والنقابات والجمعيات[8].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثالث : العلاقة بين العقوبة والتدابير الاحترازية:

بناء على ما سبق فإن التدابير الاحترازية تتفق مع العقوبة في غرضها الإصلاحي أو التأهيلي الممثل في الردع الخاص، حيث تشترك معها في العديد من الخصائص مما قلص أوجه الفرق بينهما.

ولذلك فإن معظم التشريعات الجنائية المعاصرة تتبنى النظامين معا لمكافحة الظاهرة الإجرامية، بحيث تطبق العقوبة على المجرمين المسئولين جنائيا، وتطبق التدابير الاحترازية على فاقدي الأهلية كالمجانين والأطفال غير المميزين[1].

لكن أثير خلاف بين فقهاء القانون الجنائي حول مدى إمكانية التوحيد بين العقوبة والتدبير الاحترازي في نظام واحد، وهو تساؤل طرح للبحث منذ ظهور فكرة التدابير الاحترازية، وتمت الإجابة عنه وفق اتجاهين: الأول يميل إلى توحيد العقوبة والتدبير في نظام واحد للجزاءات الجنائية، والاتجاه الثاني ينادي بضرورة المواءمة والتعايش بين العقوبة والتدبير الاحترازي في نظام مزدوج يجمع بينهما، على أن يكون لكل منهما مجاله الخاص الذي يطبق فيه.[2]

والملاحظ أن العديد من فقهاء القانون على المستوى العالمي نادوا بضرورة التوحيد بين نظام العقوبات والتدابير الاحترازية، لأن الردع الخاص يعتبر من الأعراض الرئيسة والهامة للعقوبة وهو يلتقي مع التدابير الاحترازية في أن كل منهما يهدف إلى استئصال الخطورة الإجرامية الكامنة في شخص المجرم والقضاء عليها[3].

وما نخلص إليه أن الفكر الجنائي عند غير المسلمين اتسم بالأخذ والرد والتنوع المستمر وذلك حسب تغير الظروف والزمان، ويرجع ذلك إلى الاعتقاد الخاطئ بأن الإنسانية لا تملك ما تعتمد عليه أو تنطلق منه سوى ما تنتهي إليه العقول من نظريات أو ما يقتضيه الواقع من إجراءات وهو ما أدى إلى تباين نظريات الفكر الجنائي، فقد يكتشف اللاحق من المستجدات والمعطيات ما يناقض ما انتهى إليه السابق، وغالبا ما كان الفكر الفلسفي يسبق اتجاهات السياسة الجنائية ويعطيها المسوغ والتوجيه

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

لاتخاذ ما يلزم في مواجهة ظاهرة الجريمة، لكن الواقع جعل السياسة الجنائية تتغير حسب الظروف المختلفة غير مبالية بما ساد من نظريات فلسفية، وهو ما أدى بالفكر الفلسفي إلى ملاحقة الواقع أحيان والعمل على تبريره وتوجيهه فنتج عنه تعدد النظريات مع اختلاف مضامينها، إلا أن القاسم المشترك الذي تستهدفه غالبا هو حماية المصالح من الانتهاك رغم اختلاف تلك المصالح وتقسيماتها من مدرسة إلى أخرى ومن مجتمع إلى آخر.[1]

أما التشريع الإسلامي فمنطلقاته واضحة وثوابته راسخة وأسسه قوية، ولا تفتقر إلا لبذل المزيد من الاجتهاد على بصيرة والحضور الدائم عند كل طارئ واكتشاف الخصوصية لكل زمان ومكان وتقدير المناسب لهما من الأحكام والإجراءات والتدابير، لأن الله سبحانه وتعالى أرسل الرسالات السماوية وختمها برسالة الإسلام الخالدة التي أكمل بها الدين وأتم بها النعمة وضمنها شريعة عامة مرنة صالحة لكل زمان ومكان، هدفها رعاية مصالح العباد بتحقيق العدل والأمن والرخاء لهم، ولذلك فإن التشريع الجنائي الإسلامي لا ينطلق من فراغ بل قام على أسس ربانية ثابتة سواء من حيث المصادر أو المقاصد أو القواعد.

المبحث الثاني:
التشريعات القانونية الإقليمية تجاه الجرائم الإلكترونية

أثار التطور التكنولوجي في شتى المجالات العديد من المشاكل العملية والإجرائية المتعلقة بمنع وضبط جرائم البيئة الإلكترونية نظرا لاختلافها عن الجرائم التقليدية، وأصبح لزاما على الدول أن تعمل على إيجاد الآليات التي تحمي بها هذه البيئة و توفر لها وسائل تأمينية تتفق وطبيعتها القانونية، كما خلقت هذه المسألة في بداياتها خلافا وتباينا موضوعيا لدى فقهاء القانون الجنائي في مختلف النظم حول مدى كفاءة نصوص القوانين الجنائية التقليدية في مكافحة الجرائم الإلكترونية وذلك قبل أن تتجه الآراء للحسم في عدم ملائمة النصوص القائمة لحل الإشكاليات التي تواجه الأجهزة المخولة بمنع هذا النمط الجديد من الجرائم.

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

وفي هذا الإطار فإن العديد من البلدان الأوربية كانت السباقة في إصدار التشريعات المتعلقة بمكافحة الجريمة الإلكترونية ومن بينها دولة السويد، وفرنسا، والولايات المتحدة الأمريكية، وكندا وألمانيا، لكن ما لوحظ على هذه التشريعات أنها غير جامعة بدليل أن مؤسساتها المحلية تطالب في كل عام بإدراج نماذج من السلوك الإجرامي المعلوماتي لتكون محلا للتجريم باعتبارها لم تكن متضمنة في التشريعات العقابية المعمول بها سابقا[1].

كما بادرت أيضا بعض البلدان العربية بسن تشريعات مختلفة تعالج مواضيع محددة ذات علاقة بالجريمة الإلكترونية كقانون إمارة دبي رقم 2 الصادر سنة 2002 م المتعلق بالتجارة الإلكترونية، وقانون التوقيع الإلكتروني في مصر رقم 51 الصادر في سنة 2004م، كما صدرت تشريعات مماثلة في المملكة العربية السعودية، وقطر، وسلطنة عمان، ومملكة البحرين، والأردن، والمغرب والجزائر، والمطالب التالية تعرض نماذجا من الإجراءات التشريعية المكافحة للجرائم الالكترونية في بعض الدول الأوروبية والعربية.

المطلب الأول: نماذج من الدول الأجنبية

الفرع الأول: الإطار القانوني لجرائم الكمبيوتر والانترنت في الولايات المتحدة الأمريكية.

تميزت الولايات المتحدة الأمريكية بسن تشريعات خاصة بمسائل تقنية المعلومات وما يتعلق بجرائم الكمبيوتر والانترنت، كما تميزت هذه التشريعات بمراعاتها لخصائص تطور قطاع التقنية ذاته. فعلى المستوى الفدرالي، تبلور نشاط لجنة الكونجرس الخاصة بحماية استخدام الحاسوب بإصدار قانون (غش الحاسوب وإساءة استخدامه عام 1984م) وقد ترجم باسم: (قانون الاحتيال وإساءة استخدام الحاسوب Computer Fraud and abuse Act) حيث أضيف إلى مدونة القانون الأمريكي تحت قسم الجرائم.

ويجرم هذا القانون؛ كل اتصال يحصل دون تصريح بنظام الحاسوب، كما يجرم أيضا الاتصال المصرح به والذي يستغل فيه الفاعل الحاسوب لأغراض غير مصرح بها كتعديل أو إتلاف أو تدمير أو إفشاء المعلومات المخزنة في الحاسوب، كما يعاقب هذا القانون من يرتكب فعلا من شأنه منع

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

الاستخدام المصرح به للحاسوب، وفي نفس السياق صدر أيضا " قانون أمن الحاسوب سنة 1987م" الذي يقضي باتخاذ الوكالات الفدرالية الخطوات الملائمة لتأمين وحماية أنظمة حواسيبها، حيث ينظم هذا القانون مستويات الحماية والرقابة عليها والمسؤولية عن إغفالها، وتوالت بعد ذلك العديد من التعديلات والتشريعات الفرعية والقطاعية ذات العلاقة بأمن المعلومات.

أما على مستوى الولايات، فقد سنت قوانين خاصة تم فيها تعديل قوانين العقوبات بما يكفل النص على تجريم أنشطة جرائم الحاسوب. حيث نصت قوانين بعض الولايات على المساواة بين معطيات الحاسوب والأموال المادية من حيث الحكم القانوني مما يتيح انطباق نصوص التجريم التقليدية على جرائم الحاسوب باعتبارها تستهدف المعطيات التي تتخذ حكم الأموال المادية بنص صرح القانون، ومن بين هذه الولايات ولاية ألاسكا، التي أدخل قانونها الجديد الإتلاف المعلوماتي ضمن الأموال التي تخضع لنصوص الإضرار بالمال، كما ساوى قانونها بين الغش التقليدي وغش الآلة، وكذلك ولاية فرجينيا التي نص قانونها على اعتبار وقت أو خدمات الحاسوب أو خدمات المعالجة الآلية للبيانات أو المعلومات أو البيانات المخزنة ذات الصلة بذلك هي من الأموال، وبهذا الحكم يتحقق انطباق نصوص التجريم التقليدية فيما يتصل بالاعتداء على المال.[1]

ومن المواد التشريعية المتعلقة بجرائم الكمبيوتر والانترنت على المستوى الفدرالي ومختلف الولايات ما يلي:[2]

1 ـــ في الجانب الفدرالي يمثل القسم: (18) من قانون الولايات المتحدة التشريع الرئيس لجرائم الكمبيوتر حيث تتضمن (المادة: 1030) اعتبار الأفعال التالية من قبيل الجريمة:

ـــ الدخول غير المصرح به إلى أحد أنظمة الكمبيوتر الحكومية وكشف المعلومات السرية، أو كشفها من جهة غير مصرح لها الاطلاع على المعلومات.

ـــ الدخول غير المصرح به إلى أي كمبيوتر والتوصل إلى معلومات غير مسموح الاطلاع عليها.

ـــ الدخول غير المصرح به إلى أي كمبيوتر ومن ثم ارتكاب احتيال ما.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ إلحاق أضرار جراء الدخول غير المصرح به سواء بالنظام أو البرامج أو المعلومات المخزنة فيه.

ـــ بث أو تهديد بارتكاب ضرر يطول أي كمبيوتر عبر الولايات أو يطول التجارة الأجنبية بغرض ابتزاز أموال أو منافع من أي شخص طبيعي أو معنوي.

2 ـــ وجاء في القسم:(1462) من الفصل (18) من قانون الولايات المتحدة أنه يحظر استخدام الحاسوب لاستيراد مواد مخلة بالآداب العامة إلى داخل الولايات المتحدة الأمريكية.

3 ـــ في حين أن القسم:(1463) من الفصل (18) يحظر نقل أية مواد فاحشة عبر الولايات أو الجهات الخارجية.

4 ـــ كما يجرم القسم: (2251) من ذات الفصل توظيف أي قاصر أو إغرائه في المشاركة في أنشطة جنسية بما فيها انتاج وتصوير مواد وبثها لجهات خارجية.

5 ـــ ويعتبر القسمين: (2252 ، 2252 /أ) من ذات الفصل نقل وتبادل المواد الفاحشة ذات الصلة بالأطفال جريمة.

6 ـــ أما القسم: (1028) من الفصل (18) من قانون الولايات المتحدة يعتبر إنتاج أو نقل أو إدارة جهاز يتضمن نظام الحاسوب بقصد استخدامه لتزوير الوثائق أو إنتاج وثائق تعريف مزورة جريمة، ويعتبر القسم (2319) من ذات الفصل الإخلال بحق المؤلف جريمة فدرالية.

ويتمثل الإطار العام لتشريعات الولايات المتحدة في حقل جرائم الكمبيوتر والانترنت فيما يلي:

1 ـــ **الجرائم المستهدفة للأشخاص:** تنظر العديد من الولايات في تشريعاتها إلى استخدام الكمبيوتر أو أي واسطة تقنية لارتكاب جريمة القتل على أنها مجرد وسيلة، وذلك باعتبار أن جرائم القتل تحديدا يجري العقاب فيها على النتيجة بغض النظر إلى الوسيلة المرتكبة فيها. أما ولاية (فرجينيا) فقد اعتبرت استخدام الكمبيوتر أو شبكة الكمبيوتر بدون تصريح بنية إلحاق الضرر المادي بالأفراد جريمة من بين جرائم الكمبيوتر[1]، كما اعتبرت ست عشرة ولاية من بين الولايات الأمريكية[2] أن التهديدات والمواد المثيرة للأحقاد تعد كذلك من قبيل الأفعال الجرمية على أن يكون

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

التهديد مما يمكن تطبيقه وتصديقه Credible threat لإصابة شخص ما أو الإضرار به أو بعائلته. كما تجرّم كل الاتصالات التي تتضمن مواد بذيئة بأية واسطة الكترونية تستهدف تهديد شخص أو إلحاق الضرر به أو بعائلته ويشمل ذلك استخدام الكلام الفاحش[1]، وهو ما اعتبرته محكمة نيويورك بأن هذا النص ينطبق على رسائل التهديد والذم التي ترسل عبر الانترنت[2].

2 ــ **الجرائم المتصلة بالمواد الإباحية** : تضمنت قوانين معظم الولايات مواد تجرم الأفعال التي تستهدف استغلال أو إغواء القصر أو تتعلق بدعارة الأطفال [3]، كما تجرم العديد من الولايات استخدام الكمبيوتر لجمع المعلومات حول الأطفال ومقارنتها بغرض تسهيل أو تشجيع، أو عرض، أو الحض على أنشطة جنسية محظورة تتصل بطفل ما[4]، كما منعت العديد من الولايات استخدام الكمبيوتر لإنتاج أو تخزين أو توزيع المواد الإباحية التي لها علاقة بالأطفال[5]، وتمنع أيضا معظم الولايات استخدام الكمبيوتر لإرسال المواد الفاحشة للأطفال[6].

3 ــ **جرائم الاختراق وإتلاف النظم** : هي من الجرائم التي اهتمت بها أغلب الولايات الأمريكية نظرا لما تلحقه من إضرار بالنظم والشبكات والبيانات، ولقد سطرت تشريعات تتعلق بانتهاك الحرمة Trespass ، وتشريعات تتعلق بأنشطة التخريب Vandalism ، حيث تعتبر الدخول إلى نظم الكمبيوتر أو الشبكات بدون ترخيص جريمة، وهو ما يعرف بتشريعات الـــ Hacking [7]، كما

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

نصت تشريعات تحظر هجمات التدمير وتعتبرها أكثر خطورة من أنشطة الدخول غير المصرح به، فقررت عقوبات مغلظة على الدخول غير المصرح به بقصد تدمير أو تعطيل عمل النظام أو إلحاق أي ضرر كان بالنظام أو المعطيات[1]، كما أضافت بعض التشريعات جريمة إساءة استخدام معلومات الكمبيوتر والتي يحظر في مجالها نسخ أو تلقي أو استخدام المعلومات التي تم الحصول عليها كنتيجة لإحدى جرائم الاختراق أو الهجمات التدميرية[2]. أما ولاية نيويورك فتعتبر مجرد اختراق الكمبيوتر بنية ارتكاب أي جريمة هي جريمة يعاقب عليها[3]. كما تجرم بعض الولايات إنتاج أو نقل الفيروسات والبرامج الضارة[4]، وبعضها يجرم أيضا عمليات إدخال معلومات زائفة إلى نظام كمبيوتر بهدف المساس بائتمان أي شخص كان[5]. كما يجرم عدد من الولايات الاعتداء على أجهزة الكمبيوتر أو خدمات تزويد الكمبيوتر كإحداث أي تغيير أو إتلاف للأجهزة أو الخدمات المزودة للحواسيب أو نظمها أو الشبكات[6]. و تجرم أيضا بعض الولايات كل عملية قطع أو إعاقة خدمة الكمبيوتر أو التسبب في تعطيل هذه الخدمة أو منع الدخول للنظام[7]، واعتبرت ولاية شمال كارولينا أن التهديد بتدمير الكمبيوتر أو النظام ـــ بقصد الحصول على مال أو أي منفعة كانت ـــ هي ارتكاب لجريمة كمبيوتر[8] .

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما جرمت بعض الولايات[1] عمليات الاعتداء على خصوصية الكمبيوتر أو المعلومات، أو عند استخدام الكمبيوتر والشبكات بقصد الاطلاع أو جمع المعلومات عن الموظفين أو السجلات الطبية، أو الرواتب، أو القروض، أو أي معلومات مالية شخصية مع توفر العلم بأن هذا النشاط غير مصرح به، في حين اعتبرت بعض الولايات إفشاء كلمة السر العائدة لشخص آخر جريمة كمبيوتر[2].

4 ــ جرائم الاحتيال عن طريق الحاسوب وسرقة المعطيات: جرمت غالبية الولايات المتحدة الأمريكية استخدام الحاسوب بغرض الاحتيال[3] للحصول على المال، أو المنافع، أو الخدمات عن طريق وسائل وهمية أو زائفة أو عن طريق وعود أو مظاهر كاذبة[4]، ولقد لوحظ على بعض النصوص أنها تدمج الاحتيال عن طريق الكمبيوتر ضمن نصوص الاحتيال التقليدية المقررة في قوانين هذه الولايات بدل وضع نصوص تشريعية مستقلة بشأن احتيال الكمبيوتر[5].

كما تجرم عدد من الولايات سرقة الكمبيوتر[6] المتضمنة للعديد من الأشكال؛ كسرقة المعلومات[7]، وسرقة البرامج[8]، وسرقة أجهزة الكمبيوتر[9] ، وسرقة خدمات الكمبيوتر[10] . كما جرمت غالبية الولايات استخدام الكمبيوتر لارتكاب السرقة بالمعنى التقليدي، كسرقة الممتلكات والاستيلاء على الأموال التقليدية[11].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وقد نصت عدد من تشريعات الولايات على سرقة الهوية أو وسائط التعريف، فاعتبرت من قبيل الجريمة ـــ متى توفر سبق الإصرار ـــ[1]، ورغم أن هذه التشريعات لا توصف عموما كجزء من تشريعات جرائم الكمبيوتر، ومع ذلك تم إدراجها ضمن نطاق تشريعات جرائم الكمبيوتر بسبب اتصال سرقة الهوية بأنشطة الحاسوب.

5 ـــ جرائم التزوير الإلكتروني:

تجرم بعض الولايات أنشطة التزوير عن طريق الحاسوب[2] ، حيث تفسر هذا النوع من التزوير بأنه " قيام الشخص بإنشاء أو تعديل أو إلغاء أي معطيات خاصة بأي كمبيوتر أو شبكة كمبيوتر، مما ينجم عن فعله تغيرا في الحقيقة المتعلقة بوثيقة معنوية أو تعليمات"، كما اعتبرت من قبيل جرائم الكمبيوتر حيازة أجهزة ووسائل التزوير التي تشمل الحواسيب أو معداتها أو برامجها المصممة خصيصا أو المستخدمة في ارتكاب التزوير.[3]

6 ـــ المقامرة بواسطة الحواسيب :

تعد ولاية Louisiana الوحيدة التي تجرم المقامرة بواسطة الحاسوب، ويتعلق ذلك بالقيام أو المشاركة بأي سلوك يتضمن اللعب كاليانصيب، أو المخاطرة بالبيع والشراء تحت خطر الخسارة المالية، وذلك باستخدام الانترنت[4] ، كما يجرم قانون هذه الولاية تطوير أو تزويد خدمات الحاسوب أوبرامج أو أي منتج آخر لدخول الانترنت وعرض أي نشاط يتصل بالمقامرة أو بالأعمال المكونة لهذا الفعل بقصد تحقيق مكاسب من وراء هذا السلوك.[5]

7 ـــ جرائم تعطيل الخدمات الحكومية:

يعد من الجرائم الإلكترونية في العديد من الولايات الأمريكية كل استخدام للحاسوب بغرض تعطيل تطبيق القانون أو أي خدمات حكومية[6]. كما يجرم في العديد من الولايات استخدام الكمبيوتر لتعطيل أو قطع أي خدمة أساسية، ويشمل ذلك خدمات المؤسسات العامة، والخاصة ذات

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

النفع العام، والخدمات الطبية، وخدمات الاتصال، وكافة الخدمات الحكومية، كما يشمل أيضا تعريض الأمن العام للخطر[1]. ويحظر قانون ولاية فرجينيا الغربية الدخول غير المصرح به إلى أية معلومات مخزنة داخل كمبيوتر مملوك أو متصل بجهات التشريع بالولاية[2]، كما جرم قانون جزيرة Rhode استخدام الكمبيوتر لتدمير أي دليل بقصد عرقلة أي تحقيق رسمي[3] ، واعتبرت ولاية Utah عدم الإبلاغ عن جريمة الكمبيوتر هو أيضا بمثابة جريمة.[4]

وما نخلص إليه من خلال قراءة تشريعات جرائم الكمبيوتر النافذة في مختلف الولايات المتحدة الأمريكية، وجود اختلاف حقيقي في مستويات الحماية وتحديد أنماط هذه الجرائم، إضافة إلى الاختلاف في المصطلحات المستخدمة وهو ما يؤثر على توفير الحماية ناهيك عن التباين بشأن العقوبات المقررة لهذه الجرائم، الأمر الذي يقود إلى أن هناك فجوة بين بناء وفعالية هذه التشريعات مقارنة بتشريعات الجرائم التقليدية ولعل مرد ذلك يعود إلى الطبيعة الخاصة للجرائم الإلكترونية وآثارها المختلفة مقارنة بغيرها من الجرائم كونها تمس كافة العناصر الأساسية لبناء المجتمع ونظامه السياسي والاقتصادي والاجتماعي.

الفرع الثاني : الإطار القانوني الأوروبي لجرائم الكمبيوتر والانترنت:

إدراكا من الدول الأوروبية لظاهرة جرائم الكمبيوتر التي تتوقف فعالية مكافحتها على مستوى انسجام التدابير التشريعية بين دول العالم بوجه عام، وبين الدول الأوروبية على نحو خاص وهو ما جعلها تتجه نحو توحيد التدابير التشريعية وخطط المكافحة، وقد شكلت هيئات أوروبا التشريعية والتنفيذية الأداة الفاعلة لتحقيق هذا الانسجام، كما كان للأدلة التوجيهية التي وضعها الاتحاد الأوروبي منذ الثمانينات الأثر الفاعل في تحقيق الانسجام بين التدابير التشريعية الأوروبية، ومع تطور الظاهرة وتسارعها مقارنة بالتشريعات جاءت مبادرة المجلس الأوروبي الممثلة في مشروع اتفاقية عالمية لجرائم الكمبيوتر، وهو ما سأركز عليه باعتباره في نظري الرؤية الأوسع والأحدث للإطار القانوني للحماية من جرائم الكمبيوتر دون إغفال ما سبق هذه الاتفاقية من اجتهادات على مستوى العديد من الدول الأوروبية والتي من أهمها ما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أولا: فرنســـا.

تعد فرنسا من الدول المهتمة بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية، حيث أصدرت في سنة 1985م قانونا يضيف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، والتي من بينها معاقبة أي شخص لقيامه بنشاط من شأنه التحايل على النظام الآلي بالسجن لمدة تصل إلى سنة وغرامة 100000 فرنك فرنسي[1].

وبموجب قانون العقوبات الفرنسي الصادر في عام 1998م، تم تجريم الدخول غير المشروع إلى نظام المعالجة الآلية للمعلومات أو البقاء فيها ويعاقب على ذلك بالحبس مدة تتراوح بين شهرين وعاما كاملا وبغرامة مالية من 3000 إلى 5000 فرنك فرنسي أو بإحدى هاتين العقوبتين[2]. كما صدر قانون رقم 1170 لسنة 1990م الذي احتوت مادته (28) بيان معنى التشفير وضمان سرية المعلومات والاستيلاء على المعلومات عن طريق اختراق التشفير حيث عرفت التشفير بأنه: "كل التسهيلات أو الخدمات التي تهدف إلى النقل أو التحويل، وذلك عن طريق ترتيب سرية المعلومات أو الإشارات الواضحة إلى معلومات أو إشارات مفهومة لأطراف ثالثة من خلال أجهزة أو برامج تصوره لغرض الدفاع الوطني والحفاظ على المصالح الداخلية والخارجية وأمن الدولة"[3]، ثم صدر بعد ذلك المرسوم رقم 92 ـــ 1358 في ديسمبر لسنة 1992م والمتعلق بالبلاغات والالتماسات للحصول على إذن الترميز المتعلق بالوسائل والتسهيلات، وتبين مواد هذا المرسوم تفاصيل تقديم وتصدير واستخدام خدمات أي نوع من أنواع المرافق المشفرة، وبموجبه أيضا لا تعتبر وسيلة من وسائل الترميز إذا كانت الوسيلة تتعلق بأجهزة أو برمجيات خاصة لحماية البرامج من النسخ غير المشروع استخدامها، والتي تستفيد من وسائل أو أجهزة سرية شريطة أن لا يسمح التقييد بشكل مباشر أو غير مباشر من خلال البرنامج المعني، كما عالج قانون العقوبات الفرنسي الجديد الصادر سنة 1994م تنظيم المعالجة الآلية للبيانات في المادة 323 بفقراتها الأربعة؛ حيث تجرم الفقرة الأولى الوصول أو البقاء بطريقة مخادعة في كل جزء من نظام المعالجة الآلية للمعطيات ويعاقب على ذلك بالحبس لمدة عام وبغرامة مقدرة بمائة ألف فرنك فرنسي، وإذا حصل حذف أو تعطيل أو تعديل المعطيات الموجودة في النظام أو تحريض لمجريات النظام

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

فإن العقوبة تكون الحبس لمدة عامين وغرامة مالية قدرها مائتي ألف فرنك فرنسي، أما الفقرة الثانية فقد جرمت إعاقة النظام وتزوير المعطيات والمعالجة الآلية وعقوبة ذلك الحبس لمدة ثلاث سنوات وغرامة قيمتها ثلاثمائة ألف فرنك، أما الفقرة الثالثة فجرمت كل من يدخل بطريقة مخادعة إلى معطيات نظام المعالجة الآلية أو من يحذف أو يعدل بطريقة مخادعة معطيات يحتوي عليها النظام ويعاقب بالحبس مدة ثلاث سنوات وغرامة مالية تقدر بثلاثمائة ألف فرنك فرنسي، أما الفقرة الرابعة فقد تضمنت موضوع الاشتراك والمساهمة في هذه الأفعال حيث يعاقب الشريك بنفس عقوبة الفاعل الأصلي. [1] لكن رغم أن القواعد التشريعية التي تخضع لها الجريمة المعلوماتية في القانون الفرنسي مستمدة من قواعد القانون الأوربي[2] إلا أنه يسجل بشأن القانون الفرنسي الجديد (قانون العقوبات) عدم إشارته للجرائم المالية، والجرائم التي تهدد الشخصية الفردية، والجرائم الأخلاقية ـــ الإباحية ـــ، كما أنه جاء خاليا من تجريم المقامرة عبر الانترنت والاتجار بالبشر وجرائم صناعة ونشر الفيروسات.[3]

ثانيا: المملكة المتحدة.

تصنف بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسوب حيث أقرت قانون مكافحة التزوير سنة 1981م الذي شمل في تعريفاته الخاصة تعريف أداة التزوير ووسائط التخزين الإلكتروني المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية. كما سن المشرع البريطاني قانون إساءة استخدام الحاسوب في سنة 1990م (Computer Misuse Act) الذي نتج عنه تشريع ثلاث أنواع من الجرائم الجديدة بغرض مواجهتها وهي:

أ ـــ الدخول غير المصرح به لنظام الحاسوب باعتباره النشاط الرئيسي للعبث أو التطفل.

ب ـــ الدخول غير المصرح به لنظام الحاسوب بقصد تسهيل ارتكاب فعل آخر.

جـــ ـــ التعديل أو التغيير غير المصرح به لنظام الحاسوب بقصد إضعافه أو تعطيله.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وبالرغم من أن الاستجابة البريطانية للتدابير التشريعية الجديدة في حقل تقنية المعلومات، وصفت بأنها متأخرة عن غيرها من الدول الأوروبية والأمريكية، إلا أنه بداية من سنة 1998م تشهد التجربة البريطانية تميزا ملحوظا سواء من حيث محتوى التنظيم أو الحلول التشريعية المقررة وهذا ليس في نطاق أمن المعلومات فحسب، بل في نطاق حماية البيانات الشخصية والخصوصية وتنظيم حرية البيانات والمعلومات في مختلف الفروع الأخرى لقانون تقنية المعلومات.[1]

ثالثا: ألمانيا الاتحادية.

قبل اتحاد الألمانيتين، صدر بتاريخ 15 ماي 1986م قانون مكافحة الجريمة الاقتصادية الذي بدأ سريانه في الأول من أوت 1986م، وقد جرم هذا القانون إتلاف أو محو أو تغيير أو تزوير البيانات المعالجة آليا، وشدد العقوبة بالنسبة للبيانات ذات الأهمية الأساسية لقطاع الأعمال أو السلطة الإدارية لتصل إلى حد السجن لمدة خمس سنوات وغرامة مالية، كما جرم هذا القانون الاحتيال بواسطة الحاسوب وعاقب عليه بذات العقوبة المذكورة، ويعاقب كل من تحصل على بيانات محمية بوجه خاص عن طريق الوصول غير المصرح به، كما عرف القانون الألماني العديد من المواد القانونية الرادعة للجريمة الإلكترونية وذلك تماشيا وتطور هذا النوع من الجرائم.[2]

رابعا: الدنمـــــــارك.

بتاريخ 6 جوان 1985م سن المشرع الدانماركي القانون الخاص بجريمة الحاسوب، وضمنه المواد 193 و 263 من قانون العقوبات، فيعاقب فيه مجرد الوصول إلى معلومات أو برامج الغير، وفي المادة (2/263) شدد العقوبة في حال ارتكاب فعل التوصل بغرض الإطلاع على الأسرار التجارية، كما يجرم في المادة (193) إتلاف وتعطيل أنظمة المعالجة الآلية وتخزين البيانات.[3]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثاني: نماذج من الأطر القانونية لمكافحة الجرائم الإلكترونية في الدول العربية

لقد أجرى المركز العربي للقانون والتقنية العالية دراسة بحثية وتحليلية شاملة في منتصف عام 2001م[1] بغرض الوقوف على حجم ظاهرة الجرائم الإلكترونية في الدول العربية، فوجد نحو 23% من المؤسسات محل الدراسة (عددها 1032 مؤسسة موزعة على 13 دولة عربية) قد عانت من صور جرائم الكمبيوتر، منها حوالي 59% تعرضت مواقعها الإلكترونية إلى محاولات الاقتحام أو إنكار الخدمة أو إساءة استعمال البريد الالكتروني إضافة إلى أنشطة الاعتداء على أمن التعاملات المالية في بعض المواقع، وقد أظهرت الدراسة فيما يخص إساءة استخدام البريد الالكتروني أن أكثر من 82% من الأنشطة غير المشروعة الموجهة للأنظمة مصدرها محلات الانترنت العامة Cybercafés، في حين ظهر أيضا وبنفس القدر تنامي الاهتمام بتنظيم قطاع المحلات العامة للانترنت، حيث ارتفعت نسبة الوعي لمخاطر عدم التنظيم إلى 86% عن الوضع السائد قبل عام 2001. كما احتلت هجمات الفيروسات 96% من نسبة الهجمات، و لم تتمكن الدراسة من تقديم أرقام موضوعية حول حجم الخسائر أو معدلاتها نظرا لغياب أية معايير في البيئة العربية لحساب الخسائر الحقيقية الناجمة عن هذه الجرائم[2].

و لا يعني ذلك أن الدول العربية بقيت جامدة أمام هذا النوع من الجرائم المستحدثة بل بادرت إلى التصدي لها وذلك بسن العديد من التشريعات المتعلقة بالظاهرة شأنها شأن الدول الأوروبية، وسأبين نماذج منها على سبيل المثال كما يلي:

الفرع الأول: المملكة العربية السعودية.

تعد المملكة العربية السعودية الخامسة على المستوى العالمي من حيث معدل نمو عدد الحواسيب المستخدمة، كما تعد أكبر أسواق منطقة الشرق الأوسط من حيث مبيعاتها للحواسيب[3] وتقدر نسبة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

النمو في قطاع الانترنت بالسوق السعودي أكثر من 275 %[1]، كما سجل نمو اقتناء الحواسيب بنسبة 122% سنويا[2]، إضافة إلى ذلك فإن الحواسيب ونظم المعلومات تمثل العمود الفقري لمعظم المؤسسات الحكومية والخاصة بالمملكة.

ومقارنة بالدول العربية فإن المملكة العربية السعودية تعد السباقة في إصدار التشريعات المكافحة للجرائم المعلوماتية[3]، حيث أصدرت المرسوم الملكي رقم م/17 في 8 ربيع الأول 1428هـ[4] بناء على قرار مجلس الوزراء رقم 79 المؤرخ في 7 ربيع الأول 1428 هـ، وتضمن هذا المرسوم بيان معاني المصطلحات والمسميات المتعلقة بالجرائم الإلكترونية ومنها الجريمة المعلوماتية التي عرفتها المادة الأولى بقولها "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام". كما تعاقب المادة الثالثة منه العديد من الأفعال الإجرامية بالسجن لمدة لا تزيد على سنة وبغرامة مالية لا تزيد على خمسمائة ألف ريال سعودي أو بإحدى هاتين العقوبتين لكل شخص يرتكب أيا من جرائم التنصت على ما هو مرسل عبر الشبكة المعلوماتية أو أجهزة الحاسب دون وجه حق أو التقاطه أو اعتراضه، أو الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا، أوالمساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرات وما شابهها، والتشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنية المعلومات[5]، وفي المادة الخامسة من هذا المرسوم تصل مدة السجن إلى أربع سنوات والغرامة إلى ثلاثة ملايين ريال لكل شخص يدخل بشكل غير مشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو تسريبها أو إعادة نشرها وإيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة والمستخدمة فيها أو إعاقة الوصول إلى الخدمة أوتشويشها أو تعطيلها بأي وسيلة كانت، وقد عاقبت المادة السادسة بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

هاتين العقوبتين لكل من ينتج ما يمس بالنظام العام أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي، أو إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي، أو إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس البشري أو تسهيل التعامل به أو إنشاء المواد المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة ونشرها أو ترويجها أو إنشاء موقع للاتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرق تعاطيها أو تسهيل التعامل بها.

كما بين هذا المرسوم الظروف المشددة في هذه الجرائم بالمادة م/8 ووسائل المساهمة الجنائية م/9، والعقاب على الشروع في الجرائم م/10، والحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب هذه الجرائم م/13، وجدير بالذكر أن القانون السعودي كان قد انفرد بالنص على تجريم إنتاج ونشر كل ما من شأنه المساس بالقيم الدينية والاعتداء على الأديان باستخدام وسائل تقنية المعلومات وكذلك تجريمه لإنشاء مواقع للمنظمات الإرهابية وكل ما يتعلق بها من تمويل ونشر وترويج وغيرها.

والهدف من هذا النظام القانوني هو معالجة ظاهرة الجرائم الإلكترونية من خلال وضع آلية نظامية للحد من وقوعها وذلك بتحديد الجرائم المستهدفة والعقوبات المقدرة لكل منها، مع تحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات وكل ذلك لأجل تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحواسيب والشبكات، وحماية المصلحة العامة والأخلاق والآداب العامة[1].

الفرع الثاني: دولة الإمارات العربية المتحدة.

يعتبر قانون دولة الإمارات العربية الذي ينظم مكافحة الجرائم الإلكترونية من القوانين الريادية في العالم العربي، ويعرف بالقانون الاتحادي رقم 2 الصادر سنة 2006م حيث يحمل بين طياته مواد قانونية تعاقب كل من يسيء استعمال تقنية المعلومات، وبيانه كما يلي:[2]

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

انفردت المادة الأولى بطرح المفاهيم القانونية التي تضمنها القانون لغايات مكافحة جرائم تقنية المعلومات كتعريفه للمعلومات الإلكترونية، والبرنامج المعلوماتي ونظام المعلومات الإلكتروني، والشبكة المعلوماتية والمستند الإلكتروني، وتعريفه للموقع الإلكتروني باعتباره مكان إتاحة المعلومات على الشبكة المعلوماتية، كما تطرقت المادة الأولى أيضا إلى تعريف وسيلة تقنية المعلومات والبيانات الحكومية التي تشمل بيانات الحكومة الاتحادية والحكومات المحلية والهيئات العامة والمؤسسات العامة الاتحادية والمحلية.

أما المادة الثانية فنصت على عقاب كل فعل عمدي يتوصل فيه بغير مسوغ شرعي إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة المالية أو بإحدى هاتين العقوبتين، وإذا ترتب على الفعل "إلغاء أو حذف أو تدمير أو إنشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر، وبالغرامة أو بإحدى هاتين العقوبتين" وإذا "كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة وغرامة لا تقل عن عشرة آلاف درهم أو بإحدى هاتين العقوبتين"[1]، فهذه المادة تعالج أهم الجرائم المعلوماتية بمختلف أنواعها.

وقد تعرضت المادة الرابعة لتزوير المستندات الحكومية الاتحادية أو المحلية أو ما عدا ذلك من المستندات الأخرى، حيث تنص على عقوبة السجن المؤقت لكل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفا به قانونا في نظام معلوماتي، وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأنه إحداث ضرر، كما يعاقب بالعقوبة المقررة لجريمة التزوير حسب الأحوال من استعمل المستند المزور مع علمه بتزويره.[2]

و يعاقب القانون كل من أعاق أو عطل الوصول إلى الخدمة الإلكترونية المعلوماتية، فضلا عن إيقاف هذه الخدمة أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما يعاقب بالسجن المؤقت أو الحبس كل من أتلف الفحوصات الطبية أو التشخيص الطبي أو سهل للغير القيام بذلك سواء باستعمال الشبكة المعلوماتية أو أحد وسائل تقنية المعلومات[1]، كما يجرم كل من تنصت أو التقط أو اعترض عمدا بدون مسوغ شرعي ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، حيث يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين[2].

ويعاقب بالحبس مدة لا تزيد عن سنتين وبالغرامة التي لا تزيد عن خمسين ألف درهم أو بإحدى هاتين العقوبتين كل من استعمل الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في تهديد أو ابتزاز شخص آخر لإكراهه على القيام بفعل ما أو الامتناع عنه، أما إن كان التهديد بارتكاب جناية أو بإسناد أمور تمس بالشرف أو الاعتبار فعقوبة ذلك السجن مدة لا تزيد على عشر سنوات[3].

والجدير بالذكر أن المشرع الإماراتي لم يغفل الاعتداء على الأموال عبر الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، حيث عاقب بالحبس مدة لا تقل عن سنة وبغرامة مالية لا تقل عن ثلاثين ألف درهم أو بإحدى هاتين العقوبتين لكل من استولى لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.[4]

ويعاقب المشرع الإماراتي معظم الجرائم الإلكترونية التي تقع عبر استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول دون حق إلى أرقام أو بيانات بطاقات ائتمانية أو غيرها من البطاقات الإلكترونية، حيث عاقب بالحبس مدة لا تقل عن سنة وغرامة مالية تصل إلى ثلاثين ألف درهم أو إحدى هاتين العقوبتين إذا استولى لنفسه أو لغيره على مال الغير.[5]

كما جرم المشرع كل من تعرض للشرف أو مس بالآداب العامة من خلال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، كمن ينتج أو يعد أو يهيئ أو يرسل أو يخزن بقصد الاستغلال أو التوزيع أو العرض على الغير ما من شأنه المساس بالآداب العامة فإنه يعاقب بالحبس والغرامة أو

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

بإحدى هاتين العقوبتين، وتشدد العقوبة إن كان الفعل موجها إلى الأحداث[1]. وعاقب المشرع بالسجن وبالغرامة كل من حرض ذكرا أو أنثى أو أغواه لارتكاب الدعارة أو الفجور أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وفي حال ما إذا كان المجني عليه حدثا كانت العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة.[2]

وتعاقب المادة 15 من قانون العقوبات الاتحادي بالحبس والغرامة أو بإحدى هاتين العقوبتين، كل من أساء إلى المقدسات أو الشعائر الإسلامية عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، أو أساء إلى المقدسات والشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقا لأحكام الشريعة الإسلامية، ويشمل ذلك سب الأديان السماوية المعترف بها، والحث على ارتكاب المعاصي أو الترويج لها، وتقرر العقوبة بالسجن مدة لا تزيد على سبع سنوات إذا تضمنت الجريمة مناهضة للدين الإسلامي أو جرحا للأسس والمبادئ التي يقوم عليها، أو التبشير بغير الدين الإسلامي أو الدعوة والترويج لمذهب أو فكرة تنطوي على شيء مما تقدم.

كما يعاقب القانون بالسجن المؤقت كل من قام بإنشاء موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد ترويج المخدرات أو المؤثرات العقلية وما في حكمها أو تسهيل التعامل فيها وذلك في غير الأحوال المصرح بها قانونا.[3]

بالإضافة إلى الأحكام المنصوص عليها في قانون غسل الأموال، يعاقب بالحبس مدة تصل إلى سبع سنوات، وغرامة مالية لا تزيد عن على مائتي ألف درهم، كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعا لارتكاب أي من هذه الأفعال.[4]

و لم يهمل المشرع ترويج الأفكار الهدامة والبرامج التي من شأنها الإخلال بالنظام العام والآداب العامة عن طريق استخدام شبكة المعلومات أو إحدى وسائل تقنية المعلومات وذلك بحبس الجناة مدة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

تصل إلى خمس سنوات، كما يعاقب كل من أنشأ موقعا أو نشر معلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، حيث يحبس الجاني مدة تصل إلى خمس سنوات، كما يسجل كل من قام بنشاط من شأنه المساس بطريقة مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك.[1]

ويعاقب بذات العقوبة المقررة لها، كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب أحد الجرائم المنصوص عليها في هذا القانون ووقعت الجرائم بناء على ذلك.[2]

الفرع الثالث: الجمهورية التونسية

هيأ المشرع التونسي أرضية قانونية لاستيعاب مجمل العمليات والمبادلات التجارية الإلكترونية من خلال سنه للقانون رقم 83 الصادر في 9 أوت 2000م، والذي تضمن الأحكام الخاصة بجرائم المعلوماتية والانترنت.[3]

فينص الفصل 48 من القانون المشار إليه على معاقبة كل من استعمل بطريق غير مشروع عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين 6 أشهر وعامين وبغرامة ما بين 1000 و10000 دينار تونسي أو بإحدى هاتين العقوبتين.

وبموجب الفصل 49 فإنه يعاقب كل من خالف الفصول 25 و 27 و 29 والفقرة الثانية من الفصل 31 والفصل 34 والفقرة الأولى من الفصل 35 من هذا القانون بغرامة تتراوح بين 500 و 5000دينار.

وطبقا لأحكام الفصل 50 يعاقب كل من استغل ضعف أو جهل شخص في إطار عمليات البيع الإلكتروني بدفعه الالتزام حاضرا أو آجلا بأي شكل من الأشكال، بغرامة تتراوح بين 1000 و 20000 دينار، وذلك إذا ثبت من ظروف الواقعة أن هذا الشخص غير قادر على تمييز أبعاد تعهداته أو

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كشف الحيل والخدع المعتمدة بالالتزام أو إذا ثبت أنه كان تحت الضغط مع مراعاة أحكام المجلة الجنائية.

وفي السياق نفسه ينص الفصل 51 من القانون المشار إليه على أن يعاقب كل من يخالف أحكام الفصلين 38 و 39 بغرامة تتراوح بين 1000 و 10000 دينار.

أما الفصل 52 من نفس القانون فيعاقب طبقا لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الإلكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو إلكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل.

ومع حفظ الحقوق المدنية للمتضررين طبقا لأحكام الفصل 53، يمكن للوزير المكلف بالتجارة إجراء الصلح في المخالفات المنصوص عليها بالفصل 49 من هذا القانون، والتي تتم معاينتها وفقا لأحكام هذا القانون وأيضا مع حفظ الحقوق المدنية للمتضررين، ويمكن للوزير المشرف على الوكالة الوطنية للمصادقة الإلكترونية إجراء الصلح في المخالفات المنصوص عليها بالفصل 45 من هذا القانون والتي تتم معاينتها وفقا لأحكام هذا القانون، وتكون طرق وإجراءات الصلح وفق النصوص القانونية الجاري بها العمل والمنظمة للمراقبة الاقتصادية وخاصة القانون عدد 64 لسنة 1991 المتعلق بالمنافسة والأسعار والنصوص المنقحة والمتممة له، بدون المساس بحقوق الغير.[1]

الفرع الرابع: المملكة المغربية.

سن المشرع المغربي تشريعات حديثة وأضاف نصوص أخرى لمجموعة القانون الجنائي المغربي تتلاءم وخصوصية الجريمة المعلوماتية وبيانها كما يلي:[2]

أولا– القانون المغربي رقم 3–070 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات (الفصول3–607 إلى 11–607 من مجموعة القانون الجنائي المغربي)[3]

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

يجرم المشرع المغربي كل حالة يدخل فيها شخص بدون حق إلى نظام المعالجة الآلية للمعطيات، كما يعاقب على البقاء في النظام المعلوماتي أو في جزء منه، إذا كان دخول الجاني لهذا النظام قد تم عن طريق الخطأ وهو غير مخول له حق دخوله، كما تضاعف العقوبة المقررة، إذا نتج عن فعل الدخول أو البقاء حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو اضطراب في سيره[1].

وفي الفقرة الأولى من الفصل الرابع يحدد المشرع المغربي عقوبة أشد من تلك الواردة بالفصل السابق، والتي تتعلق بالأمن الداخلي أوالخارجي للدولة أو تتعلق بأسرار مرتبطة بالاقتصاد الوطني، حيث تعتبر اعتداءا على مقومات الدولة من الناحية السياسية، أو الاجتماعية، أو الاقتصادية.

كما يشدد المشرع العقوبة في ذات الفصل إذا أدى فعل الدخول، أو البقاء غير المشروع داخل النظام، إلى تغيير أو حذف المعطيات أو اضطراب في سير النظام، وتشدد العقوبة أيضا في حالة ارتكاب الأفعال المذكورة في الفقرة الأولى من طرف موظف أو مستخدم أثناء مزاولة مهامه أو بسببها[2].

و يجرم المشرع المغربي كل فعل عمدي يؤدي إلى عرقلة سير نظام المعالجة الآلية للمعطيات، ومن صور العرقلة: إرسال الفيروسات المدمرة للمعطيات الموجودة داخل النظام.

ويعاقب كذلك من خلال هذا الفصل كل فعل يحدث خلل في نظام المعالجة الآلية للمعطيات، والخلل قد يتخذ صوراً متعددة من بينها بطئ عمل النظام المعلوماتي أو توقف المعالجة الآلية للمعطيات، ويعاقب على هذا الفعل بنفس العقوبة المقررة للعرقلة[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما يجرم المشرع في الفصل السادس كل تغيير يحصل في طريقة معالجة أو إرسال المعطيات عن طريق الاحتيال وقد حدد عقوبة الجريمة المذكورة في هذا الفصل بالحبس من سنة إلى ثلاث سنوات وغرامة مالية تتراوح بين 10000 إلى 200000 درهم مغربي أو إحدى العقوبتين [1].

ولمواجهة ظاهرة التزوير المعلوماتي، جرم المشرع المغربي تزوير أو تزييف الوثائق المعلوماتية إذا أدى ذلك إلى إحداث ضرر بالغير، كما يجرم استعمال الوثيقة المعلوماتية المزورة مع العلم بطبيعتها المزورة أو المزيفة.

و لم يحدد النص القانوني شكل الوثائق محل التزوير ليفتح مجال متابعة صنع بطاقات الائتمان المزورة، أو التزوير في مجال العقود الإلكترونية وغيرها باعتبار أن كل ذلك يصب في إطار توفير الحماية القانونية للمعاملات الإلكترونية [2].

أما فيما يخص المحاولة أو الشروع في الجرائم الواردة بهذا القانون، فقد جعل المشرع المغربي عقوبة المحاولة مماثلة لتلك المطبقة على الجريمة التامة [3].

ويجرم أيضا الاشتراك في أي عمل تحضيري من شأنه رتكاب إحدى الجرائم الإلكترونية المنصوص عليها في هذا القانون والتي تتجه فيها إرادة الجاني إلى النشاط الحقيقي للعصابة كإعداد فيروس مخصص لتدمير نظام معالجة المعطيات أو إعطاء بطاقات بنكية لمزور من أجل فك شفراتها [4].

كما يعاقب كل من صنع معدات أو أعد برامج بغرض ارتكاب إحدى الجرائم الإلكترونية، كما يعاقب أيضا كل من يحوز على هذه الوسائل أو يضعها تحت تصرف الغير [5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

واختتم المشرع المغربي فيما يخص المساس بنظم المعالجة الآلية للمعطيات بأن للمحكمة الصلاحيات في إمكانية الحكم بمجموعة من العقوبات التكميلية، كمصادرة الأدوات المستعملة في ارتكاب الجرائم المشار إليها في هذا القانون أو الأدوات المتحصل عليها من هذه الجرائم، ويمكن للمحكمة كذلك بموجب الفقرة الثانية من الفصل 11-607 الحكم على الجاني بالحرمان من ممارسة الحقوق الواردة في الفصل (40)[1] من القانون الجنائي المغربي لمدة تتراوح بين سنتين وعشر سنوات.

ويمكن للمحكمة كذلك الحكم على الجاني بالحرمان من مزاولة أية وظيفة عمومية لمدة تتراوح بين سنتين إلى عشر سنوات، كما يمكنها بعد صدور الحكم أن تحكم بإشهار الحكم الصادر بالإدانة[2].

ثانيا- القانون المغربي رقم 03ـــ03 المتعلق بمكافحة الإرهاب الالكتروني (الفصول1-218 الى9-218 من مجموعة القانون الجنائي المغربي).

يعد هذا القانون أول تشريع مغربي يشير بشكل صريح للإجرام المعلوماتي كوسيلة للقيام بأفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي يهدف إلى المساس بالنظام العام بواسطة التخويف أو الترهيب أو العنف، وقد حدد الفصل 1ـــ218 بعض الأفعال المجرمة على سبيل الحصر، من بينها الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات(الفقرة7).

كما يعاقب في الفصل2-218 أي استعمال لوسائل الإعلام ومنها الالكترونية في الإشادة بالأعمال الإرهابية، وقد حددت العقوبة بالحبس من سنتين إلى ست سنوات وبغرامة مالية تتراوح بين 10 آلاف و200 ألف درهم.[3]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثالثا–القانون رقم 03–24 المتعلق بتعزيز الحماية الجنائية للطفل والمرأة من الجرائم الإلكترونية (الفصل1–503 والفصل2–503 من مجموعة القانون الجنائي المغربي).

باستقراء مقتضيات هذا التشريع نجده يعاقب على جريمة التحرش الجنسي، وهي صيغة تسمح للقاضي بتطبيقه على كل صور التحرش الجنسي التي تقع عبر وسائل الاتصال الحديثة كالانترنت، وقد حددت العقوبة من سنة إلى سنتين حبسا والغرامة من خمسة ألاف إلى خمسين ألف درهم.[1]

ويجرم في الفصل الثاني من المجموعة الجنائية المغربية كل صور التحريض أو التشجيع أو تسهيل استغلال الأطفال الذين يقل سنهم عن ثمان عشرة سنة في مواد إباحية، وهو ما يصطلح عليه في مجال القانون المعلوماتي بالبورنوغرافية الطفولية ـــ La pornographie enfantine والذي يحقق بدون شك حماية فعالة للأطفال من مخاطر المواد الإباحية الموجودة في مواقع الانترنت على وجه الخصوص.[2]

رابعا: القانون المغربي رقم 08–09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر بتاريخ 18 فبراير 2009.[3]

تماشيا مع التوجه التشريعي في العديد من الدول التي تهدف إلى تحقيق حماية فعالة للبيانات الشخصية، أصدر المشرع المغربي القانون المذكور أعلاه ويتضمن51 مادة موزعة على ثمانية أبواب، ويشكل هذا التشريع أداة هامة لحماية الحياة الخاصة والبيانات الشخصية للمواطن المغربي خصوصا في مجال المعلوماتية، وهو ما توضحه المادة الأولى من هذا القانون التي تنص ما يلي: "المعلوميات في خدمة المواطن وتتطور في إطار التعاون الدولي. ويجب ألا تمس بالهوية والحقوق والحريات الجماعية أو الفردية للإنسان. وينبغي ألا تكون أداة لإفشاء أسرار الحياة الخاصة للمواطنين...".

كما تضمن القانون في الباب السابع الخاص بالعقوبات مجموعة من النصوص التي تحمي عمليات المعالجة وتحمي المعطيات الشخصية المعالجة، ومن أهم المواد؛ المادة53 التي تعاقب بالغرامة من 20 ألف درهم إلى 200 ألف درهم في حالة رفض المسؤول عن المعالجة حقوق الدخول أو التصريح أو

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

التعرض المنصوص عليها في المواد7 و 8 و9 من نفس القانون.

كما جرمت المادة 60 من نفس القانون عملية نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43 و44 من هذا القانون.[1]

ووفق التشريع المذكور تضاعف عقوبات الغرامة الواردة في نصوص هذا التشريع إذا كان مرتكب إحدى المخالفات شخصا معنويا دون المساس بالعقوبات التي قد تطبق على المسيرين، مع إمكانية معاقبة الشخص المعنوي بالمصادرة والإغلاق.[2]

خامسا: الحماية الجنائية للمصنفات الرقمية في إطار القانون رقم 00-02 المتعلق بحقوق المؤلف والحقوق المجاورة.

أقرت أغلب التشريعات حماية برامج الحاسب الآلي بقانون حق المؤلف، بحيث أدرجت برامج الحاسب الآلي ضمن المصنفات الفكرية الخاضعة لنصوص قانون حق المؤلف[3]، وهو ما صرح به أيضا المشرع المغربي بالنص على حماية برامج الحاسب الآلي من خلال القانون المغربي رقم 00-2 المتعلق بحقوق المؤلف والحقوق المجاورة[4]، وتبقى جريمة تقليد هذه البرامج من أهم صور الاعتداء على حقوق مؤلفيها، حيث بين المشرع المغربي أحكام هذه الجريمة من خلال الفصول 575 حتى 579 من القانون الجنائي المغربي.

ويتمثل النشاط الإجرامي في جريمة التقليد عموما في قيام الجاني بأحد أفعال التقليد المنصوص عليها الفصل 575 من القانون الجنائي المغربي، وتتحقق النتيجة الإجرامية بمجرد الانتهاء من أي فعل منه، ولا بد من توافر علاقة السببية بين النشاط الإجرامي وتلك النتيجة، وواضح هنا أن النشاط الإجرامي يجتمع فيه السلوك والنتيجة وعلاقة السببية بينهما[5]، ويعتبر محل النشاط الإجرامي في جريمة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

التقليد بصفة عامة هو المصنف المحمي[1]، ولذلك أدخل المشرع المغربي برامج الحاسب الآلي ضمن المصنفات المشمولة بالحماية بموجب قانون حق المؤلف والحقوق المجاورة[2].

سادسا: القانون المغربي رقم 53/05 المتعلق بالتبادل الالكتروني للمعطيات القانونية وبعض مقتضيات مدونة الجمارك والضرائب غير المباشرة [3].

سعى المشرع المغربي إلى تهيئة بيئة قانونية تناسب التطور في مجال المعاملات التي تتم بطرق الكترونية بغرض الانتقال من مرحلة التعامل الورقي إلى مرحلة التعامل الالكتروني، ويأتي في هذا السياق صدور القانون المغربي رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات القانونية[4]. وهو قانون ينظم المعطيات التي يتم تبادلها بطريقة الكترونية كما ينظم المعادلة بين الوثائق المحررة على الورق، وتلك المعدة على دعامة الكترونية وعلى التوقيع الالكتروني، كما يحدد هذا القانون الإطار القانوني المطبق على العمليات المنجزة من قبل مقدمي خدمات المصادقة الالكترونية وكذا القواعد الواجب التقيد بها من لدن مقدمي الخدمة المعنيين ومن لدن الحاصلين على الشهادات الإلكترونية المسلمة.

ولقد تضمن هذا القانون مجموعة من النصوص الزجرية التي تساهم في مكافحة الجرائم المعلوماتية[5]، كالإدلاء العمدي بتصاريح كاذبة أو تسليم وثائق مزورة إلى مقدم خدمات المصادقة الالكترونية[6].

كما فرض المشرع المغربي حماية خاصة لوسائل التشفير حيث يجرم استيراد أو استغلال أو استعمال إحدى الوسائل أو خدمة من خدمات التشفير دون الإدلاء بالتصريح أو الحصول على

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الترخيص[1]. ويجرم أيضا كل استعمال لوسيلة تشفير لتمهيد أو ارتكاب جناية أو جنحة أو لتسهيل ارتكابها[2].

وفيما يخص الحماية الجنائية للتوقيع الالكتروني تعاقب المادة 35 كل استعمال غير قانوني للعناصر الشخصية لإنشاء التوقيع المتعلقة بتوقيع الغير[3]. كما يحمي المشرع المغربي، من خلال المادة37، حجية الشهادة الالكترونية عبر تجريم الاستمرار في استعمالها بعد مدة صلاحيتها أو بعد إلغائها.[4]

وترفع الغرامات إلى الضعف، إذا كان مرتكب الجريمة شخصا معنويا، دون الإخلال بالعقوبات الممكن تطبيقها على المسيرين لارتكاب إحدى الجرائم المذكورة في هذا القانون.كما يمكن أن يتعرض الشخص المعنوي لعقوبات أخرى تتجلى في المصادرة أو الإغلاق[5].[6]

الفرع الخامس: الجمهورية الجزائرية

تعد الجزائر بحسب تقارير دولية خامس أكبر دولة في أفريقيا تعرضا للجرائم المعلوماتية، حيث تشير إحصائيات سابقة إلى وقوع ما بين 200 إلى 250 اعتداء يوميا على الأنظمة المعلوماتية في الجزائر[7]. ولقد استدعى تفاقم الاعتداءات على الأنظمة المعلوماتية خصوصا مع ضعف الحماية الفنية تدخلا تشريعيا صريحا، حيث بادر المشرع الجزائري إلى استدراك الفراغ القانوني من خلال التعديل الأخير لقانون العقوبات[8] عام 2004م ويتضمن المواد من 394 مكرر إلى المادة 394 مكرر7، ونصوصه كالتالي: [9]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

1 ــ يعاقب المشرع الجزائري محاولة الدخول أو البقاء غير المشروع داخل نظام المعلوماتية Accès ou le maintien frauduleux dans un système informatique. ، حيث تنص المادة394 مكرر ما يلي: يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000 دينار جزائري إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

كما تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج.

2 ــ يعاقب المشرع الإدخال غير المصرح به للمعطيات في الأنظمة الآلية، أو إزالة أو تعديل البيانات بطرق غير مشروعة، وذلك في نص المادة 394 مكرر1: التي يعاقب من خلالها بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

3 ــ وجاء في نص المادة 394 مكرر2: يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

أ ــ تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ب ــ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

4 ــ المادة 394 مكرر3 : تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.

5 ــ المادة 394 مكرر 4: يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

6 ــــ ونصت المادة 394 مكرر5: كل من شارك في مجموعة أو في اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها.

7 ــــ وتنص المادة 394 مكرر6: مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

8 ــــ أما نص المادة 394 مكرر 7: فيعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

ونظرا للاستخدام المتزايد للإنترنت في ميادين عديدة سواء على المستوى المحلي أو العالمي فإنه سجل بالمقابل زيادة في الهجمات الإلكترونية، حيث لوحظ تطورا مستمرا في أساليبها مما أصبحت تشكل تهديدا أمنيا واقتصاديا وسياسيا لاسيما مع ظهور مفهوم العصابات أو المجموعات المنظمة في مجال الجرائم الإلكترونية، مما يستوجب تحيين التشريع كلما ظهرت أنماطا جديدة من الجرائم الإلكترونية، و حرصا من المشرع الجزائري على محاصرة هذه الجرائم قام بإنجاز مشروع قانون جديد للوقاية من الجريمة الإلكترونية يتضمن 19 مادة موزعة على 6 فصول و هو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين، وقد شارك في إعداده نخبة من رجال القانون وخبراء و مهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية.

ويكتسي هذا المشروع أهمية كبيرة بالنسبة للمنظومة التشريعية الوطنية التي تعنى بمحاربة أشكال جديدة من الجرائم كونه سيساهم أكثر في التصدي لتلك الجرائم المرتبطة بالتكنولوجيات الحديثة والتي لها صلة مباشرة بالعمليات الإرهابية أو تبييض الأموال، ولقد جمع هذا المشروع بين القواعد الإجرائية المكملة لقانون الإجراءات المدنية، وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة مع التدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

كما منح نص المشروع القانوني دورا ايجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم وكشف مرتكبيها حيث تنص المادة الثالثة منه على وضع ترتيبات تقنية

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

كما نص مشروع القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ويحدد هذا القانون طبيعة الترتيبات التقنية الموضوعة لتجميع وتسجيل معطيات ذات صلة بالوقاية من الاعتداء على أمن الدولة ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

وعلى هذا الأساس، يسمح للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي. كما يسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها.

ولأجل إشراك مزودي خدمات الانترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم التكنولوجية، يلزم مشروع القانون هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات الملزمين بحفظها. وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الاتصال، والخصائص التقنية وتاريخ وزمن ومدة كل اتصال، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وعناوين المواقع المطلع عليها.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أما بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعلومات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، على أن يلتزم متعاملو الهاتف بالاحتفاظ بالمعطيات لمدة سنة ابتداء من تاريخ التسجيل.

ويتضمن مشروع القانون أيضا إجراءات عقابية لتفادي أي تهرب من التزامات القانون، حيث يعاقب الأشخاص الطبيعيين الذين يعرقلون سير التحريات القضائية عقوبة السجن من خمس إلى ست سنوات وغرامة مالية تتراوح ما بين خمسة ملايين إلى خمسين مليون سنتيم، مع معاقبة المؤسسات المخالفة بالغرامات المالية المنصوص عليها في قانون العقوبات.

ومن جهة أخرى يجبر مشروع النص التشريعي مقدمي خدمات الانترنت على الالتزام بالتدخل الفوري لسحب المحتويات التي بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين، وتخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة وإخطار المشتركين لديهم بوجودها.

ولقد صادق مجلس الأمة الجزائري في 8 جويلية 2009 بالإجماع على هذا المشروع، وبالإضافة إلى ما يتضمنه هذا القانون من أحكام خاصة بالمراقبة الإلكترونية فقد نص أيضا على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال و مكافحته تتولى تنشيط و تنسيق عمليات الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم وتم اعتماده ونشره بالجريدة الرسمية للجمهورية الجزائرية بتاريخ 5 أوت 2009. [1]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث:
التدابير والمعاهدات الدولية لمكافحة الجرائم الإلكترونية

المطلب الأول: القرارات والإجراءات الدولية لمكافحة الجرائم الإلكترونية

الفرع الأول: القرار الصادر عن الأمم المتحدة بشأن الجرائم الإلكترونية[1]

جاء إصدار هذا القرار نتيجة إيمان الدول بأن منع الجرائم الإلكترونية ومكافحتها يتطلبان استجابة في ضوء الأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به، ومن أجل ذلك فإن عناصر هذا القرار تدور حول أمور عدة هي كالتالي:[2]

1 ــ ضرورة وضع إطار قانوني دولي ملائم عن طريق بذل جميع الدول الأعضاء جهدا جماعيا.

2 ــ وجوب تكثيف الجهود المتعلقة بمكافحة الجرائم ذات الصلة بالكمبيوتر بمزيد من الفعالية التي تستدعي تطبيق جزاءات جنائية على الأصعدة الوطنية بما في ذلك النظر إذا دعت الضرورة إلى التدابير التالية:

أ ــ تحديث القوانين ومقاصدها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق الجزاءات والقوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وإدخال تغييرات مناسبة إذا دعت الضرورة إلى ذلك، بالإضافة إلى وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة للتصدي إلى هذا النوع الجديد من أشكال النظام الإجرامي.

ب ــ تحسين التدابير الأمنية والوقائية المتعلقة بالحاسوب مع مراعاة الخصوصية واحترام حقوق الإنسان وحرياته الأساسية.

ج ــ نشر الوعي لدى الجماهير والعاملين في الأجهزة القضائية والأجهزة التنفيذية بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحواسيب.

د ــ تدريب القضاة والمسئولين والأجهزة المسئولة عن منع الجرائم الاقتصادية والجرائم ذات الصلة بأجهزة الحاسوب والتحقيق فيها ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها.

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

هـ ـــ التعاون مع الهيئات المهتمة بهذا الموضوع في نص قواعد للآداب المتبعة في استخدام أجهزة الحاسوب والنفاذ إلى الشبكات.

و ـــ اعتماد سياسات بشأن ضحايا الجرائم المتعلقة بالكمبيوتر تنسجم مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجرام والتعسف في استعمال السلطة، وتدابير تشجع الضحايا على إبلاغ السلطات المختصة بهذه الجرائم.[1]

الفرع الثاني: المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات[2]

أوصى المؤتمر بمجموعة من القواعد الموضوعية والإجرائية بشأن جرائم الكمبيوتر وهي كما يلي:[3]

أولا: القواعد الموضوعية

تتضمن القواعد الموضوعية النص على قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر وهي كما يلي:

1 ـــ جريمة الاحتيال أو الغش المرتبط بالكمبيوتر: وتشمل الإدخال والإتلاف والمحو لمعطيات الكمبيوتر أو برامجه، أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق الخسارة بأي شخص كان بقصد جني الفاعل منافع اقتصادية له أو للغير.

2 ـــ جريمة التزوير الإلكتروني: وتشمل إدخال أو إتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات عن طريق الكمبيوتر.

3 ـــ جريمة الإضرار بالبيانات والبرامج: وتشمل المحو والإتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه.

4 ـــ جريمة تخريب وإتلاف الكمبيوتر: وتشمل كل فعل يؤدي إلى تعطيل وظيفة من وظائف الكمبيوتر أو نظام الشبكات.

5 ـــ جريمة الدخول غير المصرح به: وهو التوصل أو الولوج دون ترخيص إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الحماية الأمنية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

6 ـــ جريمة الاعتراض غير المصرح به: وهو الاعتراض بواسطة وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات.

ثانيا: القواعد الإجرائية

تتضمن القواعد الإجرائية مجموعة من الأسس الواجب مراعاتها في مكافحة الجرائم المتعلقة بالكمبيوتر ممثلة في:

1 ـــ وجوب تحديد السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وخاصة ضبط الأشياء غير المادية وتفتيش شبكات الحاسوب.

2 ـــ وجوب إتاحة قدر كبير من التعاون الفعال من طرف المجني عليهم، والشهود، وغيرهم من مستخدمي تكنولوجيا المعلومات، مما يسمح باستخدامها للأغراض القضائية في حال هذه الجرائم.

3 ـــ السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسب ذاته، أو بينه وبين نظم الحواسيب الأخرى، مع استخدام الأدلة المحصل عليها في الإجراءات أمام المحاكم.

4 ـــ وجوب الإحاطة بكل المسائل المرتبطة ببيئة تكنولوجيا المعلومات، كالتجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسارة الاقتصادية، كلفة إعادة بناء قواعد البيانات إلى وضعها السابق قبل إجراء أي تفتيش أو تحقيق.

5 ـــ القواعد القائمة في مجال الإثبات الإلكتروني ومصداقية الأدلة، وما يلحقها من مشاكل عند تطبيقها، بحيث ينبغي إدخال بعض التغييرات التشريعية في حالة الضرورة.

الفرع الثالث: مركز الشكاوى العالمي الخاص بجرائم الانترنت[1]

تعود فكرة تأسيسه إلى سنة 1998م، وهو يعرف باسم (IC3) كناية عن نظام تبليغ وإحالة شكاوى الناس في العالم أجمع ضد جرائم الانترنت حيث يخدم المحللين والجمهور ووكالات فرض تطبيق القوانين الأمريكية والدولية التي تحقق في جرائم الانترنت[2]، ويتكون المركز من موظفين فدراليين ومحللين من القطاع الأكاديمي وقطاع صناعة الكمبيوتر وخدمات الانترنت الذين بدورهم يتلقون الشكاوى المتعلقة بجرائم الانترنت من الجمهور ثم يقومون بتبويبها وإحالتها إلى وكالات

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

تطبيق القانون الفدرالية والمحلية التابعة للولايات المتحدة وإلى أجهزة تطبيق القانون الدولية أو الوكالات التنظيمية أوفرق العمل التي تشارك فيها عدة وكالات للقيام بالتحقيق فيها.

ولذلك فإنه بإمكان كل فرد من كافة أنحاء العالم أن يقدم شكوى إلى مركز الشكاوى الخاص بجرائم الانترنت العالمي على الموقع الإلكتروني الرسمي (http://www.ic3.gov)، حيث يقوم المعني بتسجيل معلوماته الخاصة على الاستمارة الإلكترونية للشكاوى، ثم يدلي إن أمكن بالبيانات الخاصة بالشخص أو المنظمة المشتبه بقيامها بنشاط إجرامي، إضافة إلى التفاصيل المتعلقة بكيفية وقوع الجريمة حسب اعتقاد المعني ووقت وقوعها وسببها، وإلى أي معلومات أخرى تدعم الشكوى[1]، وعلى إثرها يقوم المركز بجمع الشكاوى وتحليل مدى خطورتها ومقارنتها بالشكاوى التي قد تكون لها علاقة حيث تتحول الجريمة عندئذ إلى قضية أكثر أهمية ويصبح بإمكان وكالات تطبيق القانون التحقيق فيها.

ونظرا لحاجة مركز الشكاوى IC3 في بعض الأحيان إلى تعقب التحقيقات المستعجلة في القضايا التقنية المعقدة، فقد قام بإنشاء مكتب فرعي يعمل على هذا الغرض في بيترسبرغ بولاية بنسلفينيا أطلق عليه اسم "وحدة مبادرات جرائم الإنترنت ودمج مواردها" (CIRFU) حيث يقوم محللو هذه الوحدة بإلغاء مسارات التحقيق الخاطئة ويقومون بغربلة أدلة القضية وتنقيحها قبل إحالتها إلى وكالات تطبيق القوانين أو فرق العمل الخاصة المحلية أو الدولية[2]. وتحظى هذه الوحدة (CIRFU) بالدعم من أكبر الشركات المستهدفة بالجرائم الإلكترونية المعروفة على المستوى العالمي، كما انضم إلى هذه الوحدة محققون ومحللون ينتمون إلى هذه الشركات بغرض تحديد اتجاهات وتكنولوجيات جرائم الإنترنت ولجمع المعلومات لإعداد ملفات القضايا القانونية الهامة، ولمساعدة وكالات تطبيق القانون في جميع أنحاء العالم على اكتشاف جرائم الانترنت ومحاربتها، إضافة إلى إمكانية التوصل إلى معرفة المصدر الذي تنبثق عنه الجريمة، ومن يقف وراءها ومن ثم إلقاء القبض على المتورطين[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثاني: الاتفاقية الأوروبية ــ بودابيست[1] ــ لمكافحة الجرائم الإلكترونية.

الفرع الأول: منطلقات الاتفاقية ومرجعياتها [2]

جاء في مقدمة الاتفاقية ضرورة الحاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر وآثارها الخطيرة على الدول، خاصة في ظل شيوع شبكات المعلومات وفي ظل التوسع والنماء الكبير لأنظمة الحوسبة المفتوحة ونقل وتدفق المعلومات. كما أكدت المقدمة على أهمية مكافحة كافة الأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الكمبيوتر وهي؛ السرية confidentiality، وسلامة المحتوى integrity ، وتوفر المعلومات والنظم availability وهذا في الحقل الموضوعي ــ نصوص التجريم الموضوعية ــ، أما في الحقل الإجرائي فقد أكدت مقدمة الاتفاقية على اتخاذ التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على أهمية التعاون المحلي والإقليمي والدولي مع وجوب إقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الأساسية والسيادة.

و يمكن تلخيص منطلقات وأهداف ومرجعيات مواد الاتفاقية كما يلي:

1 ــ السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية .

2 ــ التأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والانترنت وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة جرائم الكمبيوتر والانترنت.

3 ــ ضرورة تفعيل خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات، بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة، والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة في ميدان جرائم الكمبيوتر على المستوى الوطني والدولي.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

4 ـــ تحقيق التوازن بين حماية حقوق الإنسان الأساسية (المعترف بها بموجب اتفاقية مجلس أوروبا لحماية حقوق الإنسان وحريته الأساسية لعام 1950م، والعهد الدولي للحقوق المدنية والسياسية لعام 1966م، والاتفاقيات العالمية الأخرى في ميدان حقوق الإنسان) وتحديدا الحقوق المتصلة بالرأي، وحرية الوصول للمعلومات، وحرية البحث والتلقي والنقل للمعلومات والأفكار ، وبين الحق في الخصوصية وفي حيازة المعلومات والإفادة من عناصر الملكية الفكرية لها.

وتنطلق الاتفاقية من بين مرجعياتها من أحكام اتفاقية مجلس أوروبا لعام 1981 م بشأن حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، ومن اتفاقية الأمم المتحدة لعام 1989 م بشأن حقوق الطفل، واتفاقية منظمة العمل الدولية لعام 1999م بشأن عمالة الأطفال، وكذلك من الاتفاقيات الثنائية والجماعية المبرمة بين الاتحاد الأوروبي والدول الأخرى بشأن التعاون القضائي والأمني وهذا من أجل تحقيق فعالية في ميدان مكافحة جرائم الكمبيوتر العابرة للحدود وأنشطة التحقيق والمقاضاة لهذه الجرائم.

كما تنطلق أيضا من الجهود الدولية والإقليمية وتحديدا أنشطة الأمم المتحدة ، ومنظمة التعاون الاقتصادي والتنمية OECD ، والاتحاد الأوروبي ومجموعة دول الثمانية، كما تعتمد الاتفاقية على ما سبق إقراره من أدلة إرشادية، وتوصيات تشريعية منذ عام 1985م والممثلة بالدليل الأوروبي الإرشادي لعام 1985 م المتعلقة بحقل أنشطة التقاط الاتصالات، وتوصيات عام 1988م بشأن القرصنة في ميدان حق المؤلف والحقوق المجاورة، وتوصية 1987 م المتعلقة استخدام البيانات الشخصية في القطاع العام، وتوصيات 1995 م بشأن حماية البيانات الشخصية في حقل الاتصالات وخدمات الهاتف، وتوصيات عام 1989 بشأن التوجيهات للمشرعين حول تعريف وتحديد جرائم الكمبيوتر وتوجيهات عام 1995 المتعلقة بمشكلات القانون الإجرائي المتصلة بتقنية المعلومات، وقرار مجلس وزراء العدل الأوروبي الصادر عام 1997 م الذي أوصى بدعم وتبني أنشطة اللجنة الأوروبية لمشكلات الجريمة في حقل جرائم الكمبيوتر من أجل توفير الحماية من جرائم الكمبيوتر سواء بالنسبة للقواعد الموضوعية أو الإجرائية، وقرار وزراء العدل الصادر عام 2000م بشأن تشجيع أنشطة التعاون والتوصل إلى حلول موحدة ومناسبة لأكبر عدد من دول العالم في حقل مكافحة جرائم.[1]

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

الفرع الثاني: المفاهيم الموضوعية للاتفاقية

احتوى الفصل الأول في المادة الأولى من الاتفاقية على مجموعة من التعريفات definitions، وهو ما ميّز هذا المادة بأهمية استثنائية من جهة توحيد التعريفات بعدما ظهر التناقض والتباين في تشريعات جرائم الكمبيوتر التي جرى سنها في أوروبا، وأمريكا، واستراليا، وعدد من دول شرق آسيا.

كما تضمن الفصل الثاني من الاتفاقية أقساما ثلاثة، تطرق القسم الأول منها إلى التدابير الموضوعية، والثاني حول التدابير الإجرائية ، والثالث حول الاختصاص، ومن خلال هذا الفصل تكون الاتفاقية قد قدمت الإطار القانوني للتدابير التشريعية الموضوعية والإجرائية المتعين اتخاذها لمواجهة جرائم الكمبيوتر والانترنت .

واستحدثت الاتفاقية تقسيما جديدا نسبيا بشأن جرائم الكمبيوتر وأحكامها حيث تضمن أربع تصنيفات رئيسة لجرائم الكمبيوتر، وصنف خامس تعلق بأحكام المساهمة والعقوبات للتصنيفات الأربعة، وذلك على النحو التالي:

التصنيف الأول: الجرائم التي تستهدف عناصر أمن المعلومات وهي السرية والسلامة وتوفر معطيات نظم الكمبيوتر ، وتشمل جريمة الدخول غير القانوني (مادة 2) والاعتراض غير القانوني (مادة 3) والتدخل في المعطيات (مادة 4) والتدخل في نظم الحاسوب (مادة 5) وإساءة استخدام الأجهزة (مادة 6) .

التصنيف الثاني: الجرائم المرتبطة بالكمبيوتر، وتشمل التزوير المرتبط بالكمبيوتر (مادة 7) والاحتيال المرتبط بالكمبيوتر (مادة 8) .

التصنيف الثالث: الجرائم المرتبطة بالمحتوى ، وتشمل صورة واحدة من هذه الجرائم هي جرائم دعارة الأطفال (المادة 9) .

التصنيف الرابع: الجرائم المرتبطة بحق المؤلف والحقوق المجاورة، وتشمل الجرائم الجنائية التي تعد اعتداءا على المصنفات المحمية بحق المؤلف والحقوق المجاورة (مادة 10) .

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

التصنيف الخامس: المساهمة الجرمية والعقوبة، ويعالج هذا الجزء الشروع attempt والمساعدة aiding والتحريض abetting (مادة 11) ومسؤولية الأشخاص المعنوية corporate liability (مادة 12) ومعايير العقاب sanctions and measures (مادة 13) .

واستنادا إلى المواد المشار إليها (2ـــ13) فان الاتفاقية تلزم الدول الأعضاء ـــ الدول الأوروبية وأية دولة توقع عليها أو تنضم إليها من خارج المجموعة الأوروبية ـــ باتخاذ التدابير التشريعية والإجراءات الملائمة لتجريم تسع ظواهر في ميدان جرائم التقنية وهي:

1 – الدخول غير القانوني المتعمد: حيث استخدمت الاتفاقية هذا التعبير illegal access والمقصود به الدخول غير المصرح به unauthorized access ، وذلك بالدخول المتعمد إلى أي نظام كمبيوتر أو جزء منه دون حق أو إذن، سواء أكان بنية انتهاك وسائل الأمن infringing security mesures أو بنية الحصول على معطيات الكمبيوتر أو لأية نية غير مشروعة (مادة 2) .

2 – الاعتراض غير القانوني المتعمد illegal interception: وهو اعتراض بدون حق للبيانات الخاصة non-public المرسلة إلى أو من نظام كمبيوتر، ويندرج ضمن هذا العنصر اعتراض الذبذبات الكهرومغناطيسية المنبعثة من نظام كمبيوتر والتي تحمل مثل هذه المعطيات (مادة 3).

3 – التدخل المتعمد في المعطيات interference data ، وإتلافها damaging أو حذفها deletion ، أو تشويهها وإفسادها deterioration ، أو تغيرها أو تعديلها alteration ، أو تعطيلها supperession ، وقد ذهبت لجنة الخبراء إلى أن تعديل البيانات يشمل خلطها (الغش)، أما تعطيل البيانات فيتعلق بإجراءات منع وصولها إلى العنوان المرسل إليه كحذف جزء منها على نحو لا يتيح وصولها إلى الموضع الفيزيائي المطلوب، أو تصبح غير قادرة على ذلك أو منع الغير من الوصول إليها(المادة 4) .

4 – التدخل العمدي في الأنظمة system interference وذلك بارتكاب ذات الأفعال المشار إليها في المادة 4 ، المتعلقة بالتدخل في المعطيات لتعطيل أداء وعمل الأنظمة بالتدمير، أوالحذف والتعديل والتعطيل، إضافة وسيلة البث أو الإرسال inputting or transmitting (مادة 5).

5 – إساءة استخدام الأجهزة Misuse of devices ، (مادة 6)، وتشمل الأفعال الأولى المنصوص عليها في الفقرة الأولى من المادة السادسة، كالإنتاج المتعمد production ، أو بيع sale أو شراء procurement ، أو استخدام use ، أو استيراد import أو توزيع distribution وغير ذلك من

(1) الإحالات في النسخة المطبوعة.
(2) الإحالات في النسخة المطبوعة.

.../.....

الوسائل والأدوات التي يكون الهدف من ورائها ارتكاب أي جريمة من الأفعال المنصوص عليها في المواد 2ـــ5 المشار إليها أعلاه، بالإضافة إلى كلمات المرور السرية computer password ، ورموز الدخول access code أو أية معطيات مشابهة تتيح اختراق نظام الكمبيوتر أو الدخول إليه أو إلى أي جزء منه بنية ارتكاب أي فعل من الأفعال المنصوص عليها في المواد 2–5 ، كما تشمل هذه الجريمة وفق الفقرة الثانية من المادة 6 حيازة أي عنصر أو أداء مما ورد ذكره في الفقرة الأولى أعلاه بنية ارتكاب أي من الأفعال المشار إليها في المواد 2–5 من الاتفاقية .

6 – التزوير المتعمد باستخدام الكمبيوتر computer-related forgery ، وذلك بإدخال، أو تعديل، أو حذف، أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات مزورة على أنها بيانات أصلية، وبغض النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة فيحق للدولة أن تدين نية أو قصد الغش لقيام المسؤولية الجنائية (مادة 7).

7 – الاحتيال المتعمد باستخدام الكمبيوترcomputer-related fraud على نحو يسبب خسارة الغير لممتلكاته عن طريق إدخال أو حذف أو تعديل أو كتم بيانات الكمبيوتر، أو من خلال التدخل في عمليات نظام الكمبيوتر أو برامجه بنية الحصول على منفعة اقتصادية economic benefit لنفسه أو لغيره (مادة 8) .

8 – الجرائم المرتبطة بدعارة الأطفال offences related to child pornography ، وهي الجريمة الوحيدة التي تصنف لدى الاتفاقية ضمن جرائم المحتوى بالرغم من أن العديد من الدول اتجهت إلى تصنيف أفعال أخرى ضمن هذا النوع من الجرائم كالمقامرة على الشبكة، أو إثارة الأحقاد والفتن وغيرها، وقضت الاتفاقية في المادة التاسعة منها بوجوب اتخاذ الدولة المنظمة للاتفاقية التدابير التشريعية لتجريم قيام أي شخص متعمدا بعرض offering ، أو توزيع distributing ، أو نقل transmitting أو غير ذلك من الأفعال التي من شأنها توفير المواد الإباحية المتعلقة بالأطفال child pornography من خلال نظام الحاسوب، وتجريم إنتاج مواد دعارة الأطفال بغرض التوزيع عبر نظام الحاسوب، وذهب فريق الخبراء إلى أن عرض المواد الإباحية يتضمن كذلك إعطاء معلومات حول وسائل العرض والاتصال لهذه المواد وكذلك ربط المواقع بوصلات إلى مواقع إباحية، كما ثار جدل حول مفهوم المواد الإباحية المتعلقة بالأطفال وما تشمله حيث اقترح ترك ذلك للنظم الوطنية حسب قواعد النظام

(1) الإحالات في النسخة المطبوعة.
(2) الإحالات في النسخة المطبوعة.

.../.....

والآداب العامة المعمول بها، وفي ضوء الخلاف حول المحتوى ونطاقه جرى الاتفاق على معايير الحد الأدنى التي نص عليها في الفقرتين الثانية والثالثة من ذات المادة ، فقضت الفقرة الثانية من المادة 9 على أن مواد دعارة الأطفال تشمل أية مواد تظهر بشكل مرئي قيام القاصر بتصرفات جنسية أو ظهور أي شخص باتصال أو تصرف جنسي مع قاصر، وكذلك الصور الواقعية realistic التي تمثل أو تظهر قاصرا يقوم بتصرف جنسي. أما الفقرة الثالثة، فقد قررت أن المقصود بالقاصر minor يحدد تبعا للقانون الداخلي للدول الأعضاء على أن يتضمن في جميع الأحوال الأطفال دون سن الثامنة عشرة، وللدول الأعضاء اعتماد حد أدنى أقل على أن لا يقل عن 16سنة (المادة 9 بفقراتها الثلاث).[1]

9 – الجرائم المرتبطة بحق المؤلف : copyright and related offences جاء في المادة 10 بفقرتيها الأولى والثانية؛ وجوب اتخاذ الدول المنظمة تدابير تشريعية تجرم الاعتداء على حق المؤلف أو الحقوق المجاورة وفقا لما تحدده القوانين الوطنية للدول الأعضاء الموافقة مع اتفاقية بيرن لحماية المصنفات الأدبية والفنية واتفاقية تربس trips ، واتفاقية الوايبو لحق المؤلف WIPO copyright treaty واتفاقية الوايبو للاداء والفنوغرامات WIPO performances and phonograms treaty ، على أن تكون هذه الأفعال قد ارتكبت عمدا intentionally وبغرض تجاري commercial seale وباستخدام نظام الكمبيوتر.

وقد تناولت الاتفاقية في المادة الحادية عشرة القواعد العامة المتعلقة بالمساهمة الجنائية والعقوبة بشأن الجرائم المشار إليها في المواد من 2 ـــ 10 ، وفرضت على الدول الأعضاء اتخاذ تدابير تشريعية للنص على مسؤولية الشروع والتدخل والتحريض في ارتكاب هذه الجرائم أو ما تختاره الدولة منها ، وكذلك النص على مسؤولية الأشخاص المعنوية عن الأفعال التي ترتكب لمصلحة الشخص المعنوي من قبل الشخص الطبيعي الذي يتصرف لمصلحته استنادا إلى تمثيل قانوني أو باعتباره مناطا به اتخاذ القرار عن الشخص القانوني أو لأنه خاضع لسلطته بما في ذلك افعال التحريض والتدخل والمساعدة الجنائية، وكذلك مسؤولية الأشخاص الطبيعية والمعنوية عن غياب أو تخلف الرقابة والإشراف والتحكم بتصرفات الأشخاص الطبيعيين، أما بالنسبة للعقوبات والتدابير فقد أوجبت الاتفاقية على الدول المنضمة إقرار العقوبات الملائمة والفعالة لهذه الجرائم بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعيين والغرامات المالية بالنسبة للأشخاص المعنوية.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

ومنا نخلص إليه أن هذه الاتفاقية تقدم لأول مرة إطارا لتحديد قائمة جرائم الكمبيوتر وأنماطها، فبالرغم من الجهود التشريعية والتدابير الإقليمية والدولية على مدى السنوات الثلاثين الماضية لم تتوفر رؤية شاملة أو إطار واضح يحدد قائمة الجرائم أو بيّن أساس التقسيم، ولهذا فان أهم ما يسجل لهذه الاتفاقية أنها تطرح إطارا للتقسيم والتحديد بشأن القواعد الموضوعية لجرائم الكمبيوتر والانترنت.

المطلب الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1]

انبثقت هذه الاتفاقية برغبة من الدول العربية من أجل تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات المهددة لأمنها ومصالحها وسلامة مجتمعاتها، واقتناعا من هذه الدولة بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، والتزاما بالمبادئ الدينية والأخلاقية السامية ولاسيما أحكام الشريعة الإسلامية التي تنبذ كل أشكال الجرائم، ومراعاة للنظام العام لكل دولة، فقد وقعت معظم الدول الأعضاء على هذه الاتفاقية كما شهدت إقرارا متواصلا من الدول الأعضاء ابتداء من تاريخ إصدارها نظرا لاستفحال ظاهرة الجريمة الإلكترونية في البلدان العربية[2].

الفرع الأول: المفاهيم الموضوعية للاتفاقية

تحتوي هذه الاتفاقية على خمسة فصول شملت ثلاثة وأربعون مادة (43)، فتطرق الفصل الأول منها إلى الأحكام العامة المفسرة لأهداف الاتفاقية ومصطلحات تعريفية لتقنية المعلومات ومزود الخدمة والبيانات، والبرنامج المعلوماتي، والنظام المعلوماتي، والشبكة المعلوماتية والموقع، والالتقاط، ومعلومات المشترك، كما تطرق أيضا إلى مجالات تطبيق الاتفاقية المتعلقة بجرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، منوهة في ذلك إلى صون السيادة الإقليمية وعدم التدخل في الشؤون الداخلية للدول الأخرى.[3]

وتطرق الفصل الثاني من الاتفاقية إلى تجريم الظاهرة ضمن سبعة عشر مادة وبيانها كما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المادة الخامسة: إلزام كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقا لتشريعاتها وأنظمتها الداخلية.

المادة السادسة: جريمة الدخول غير المشروع وتشمل؛

1 ـــ الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

2 ـــ تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ ـــ محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

ب ـــ الحصول على معلومات حكومية سرية.

المادة السابعة: جريمة الاعتراض غير المشروع؛ ويقصد به الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

المادة الثامنة: الاعتداء على سلامة البيانات وذلك عن طريق؛

1 ـــ تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.

2 ـــ للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تسبب بضرر جسيم.

المادة التاسعة: جريمة إساءة استخدام وسائل تقنية المعلومات؛

1 ـــ إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ ـــ أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب ـــ كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ــ حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

المادة العاشرة: جريمة التزوير المتمثلة في استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

المادة الحادية عشرة: جريمة الاحتيال كالتسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:

1 ــ إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

2 ــ التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

3 ــ تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

المادة الثانية عشرة: جريمة الإباحية التي تشمل:

1 ــ إنتاج أو عرض، أو توزيع، أو توفير، أو نشر، أو شراء، أو بيع، أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.

2 ــ تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.

3 ــ يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

المادة الثالثة عشرة: الجرائم الأخرى المرتبطة بالإباحية وهي المقامرة والاستغلال الجنسي.

المادة الرابعة عشرة: جريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.

المادة الخامسة عشرة: الجرائم المتعلقة بالإرهاب والمرتكبة بوساطة تقنية المعلومات وهي:

1 ــ نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

2 ــ تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

3 ــ نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

4 ــ نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

المادة السادسة عشرة: الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بوساطة تقنية المعلومات:

(1) الإحالات في النسخة المطبوعة.
(2) الإحالات في النسخة المطبوعة.

.../.....

1 ــ القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

2 ــ الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.

3 ــ الاتجار بالأشخاص.

4 ــ الاتجار بالأعضاء البشرية.

5 ــ الاتجار غير المشروع بالأسلحة.

المادة السابعة عشرة: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، وانتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي.

المادة الثامنة عشرة: الاستخدام غير المشروعة لأدوات الدفع الإلكترونية.

1 ــ كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.

2 ــ كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.

3 ــ كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

4 ــ كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

المادة التاسعة عشرة: الشروع والاشتراك في ارتكاب الجرائم.

1 ــ الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف.

2 ــ الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية.

3 ــ يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المادة العشرون: المسؤولية الجنائية للأشخاص الطبيعية والمعنوية، بحيث تلتزم كل دولة طرف مع مراعاة قانونها الداخلي بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا.

المادة الحادية والعشرون: تشديد العقوبات على الجرائم التقليدية المرتكبة بوساطة تقنية المعلومات.

بمعنى أن كل دولة طرف تلتزم بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

وتضمن الفصل الثالث من الاتفاقية الأحكام الإجرائية وتشمل؛ نطاق تطبيق الأحكام الإجرائية كأن تتبنى كل دولة طرف في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من الاتفاقية[1]، كما تشمل التحفظ العاجل على البيانات المخزنة في تقنية المعلومات[2]، والتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين بحيث تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات[3]، كما يشمل هذا الفصل أيضا قضية أمر تسليم المعلومات وتفتيش المعلومات المخزنة وضبطها، إضافة إلى التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات[4].

أما الفصل الرابع من الاتفاقية تطرق إلى ضرورة الالتزام بالتعاون القانوني والقضائي كتسليم المجرمين، والمساعدة المتبادلة لغايات التحقيقات أو جمع الأدلة الالكترونية، ومساعدة الدول الأخرى في حال حصول أي دولة طرف على المعلومات العرضية، وكل ذلك يتم وفق إطار احترام السيادة والأمن والمصلحة الأساسية لكل دولة طرف بحيث يحق لكل دولة رفض المساعدة إذا ارتأت بأن هذه الأخيرة قد تخل بسيادتها.[5]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أما الفصل الخامس من الاتفاقية فجاءت فيه الأحكام الختامية التالية:

1 ــ تعمل الجهات المختصة لدى الدول الأطراف على اتخاذ الإجراءات الداخلية اللازمة لوضع هذه الاتفاقية موضع التنفيذ.

2 ــ تكون هذه الاتفاقية محلا للتصديق عليها أو قبولها أو إقرارها من الدول الموقعة، وتودع وثائق التصديق أو القبول أو الإقرار لدى الأمانة العامة لجامعة الدول العربية في موعد أقصاه ثلاثون يوما من تاريخ التصديق أو القبول أو الإقرار، وعلى الأمانة العامة إبلاغ سائر الدول الأعضاء والأمانة العامة لمجلس وزراء الداخلية العرب بكل إيداع لتلك الوثائق وتاريخه.

3 ــ تسري هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية.

4 ــ يجوز لأية دولة من دول الجامعة العربية غير الموقعة على هذه الاتفاقية أن تنضم إليها، وتعتبر الدولة طرفا في هذه الاتفاقية بمجرد إيداع وثيقة التصديق أو القبول أو الإقرار أو الانضمام لدى الأمانة العامة لجامعة الدول العربية، ومضي ثلاثين يوما على تاريخ الإيداع.

5 ــ مع مراعاة ما نصت عليه الفقرة (3) من المادة التاسعة عشرة، إذا تعارضت أحكام هذه الاتفاقية مع أحكام أية اتفاقية خاصة سابقة يطبق النص الأكثر تحقيقا لمكافحة جرائم تقنية المعلومات.

6 ــ لا يجوز لأية دولة من الدول الأطراف أن تبدي أي تحفظ ينطوي على مخالفة لنصوص هذه الاتفاقية أو خروج على أهدافها.

7 ــ يجوز للدولة الطرف أن تقترح تعديل أي نص من نصوص هذه الاتفاقية وتحيله إلى الأمين العام لجامعة الدول العربية الذي يقوم بإبلاغه إلى الدول الأطراف في الاتفاقية لاتخاذ قرار باعتماده بأغلبية ثلثي الدول الأطراف، ويصبح هذا التعديل نافذا بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق أو القبول أو الإقرار من سبع دول أطراف لدى الأمانة العامة لجامعة الدول العربية.

8 ــ يمكن لأي دولة طرف أن تنسحب من هذه الاتفاقية بناء على طلب كتابي ترسله إلى الأمين العام لجامعة الدول العربية، ويترتب أثر الانسحاب بعد مضي ستة أشهر من تاريخ إرسال الطلب إلى الأمين العام لجامعة الدول العربية.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وما يمكن استخلاصه من هذا المبحث أنه رغم المعاهدات والاقتراحات التي تنادي بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية، إلا أن الواقع يسجل عوائق عديدة تحول دون تحقيق هذا التعاون أهما:

1 ــ عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي: فلم تتفق الأنظمة القانونية في بلدان العالم على صور محددة يندرج في إطارها ما يسمى "بإساءة استخدام نظم المعلومات الواجب إتباعها"، كما ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه وهو نتاج طبيعي لقصور التشريع ذاته في كافة بلدان العالم تجاه مسايرة سرعة التقدم المعلوماتي ومن ثم الجريمة المعلوماتية، ودليل ذلك لا تزال دول لم تصدر بعد قانونا يتعلق بالجريمة الإلكترونية، ولا زال الخلاف يدور هل من الأفضل تعديل التشريعات العقابية القائمة كي تستوعب نماذج الجريمة المعلوماتية، أم تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه الأنشطة من السلوك وتجرمها بوصفها أقرب ما تكون إلى حق المؤلف، أم يكون من الملائم إصدار تشريعات جديدة خاصة بالجريمة المعلوماتية، ولم يقف الخلاف عند هذا الحد بل إن ما يراه البعض مباحا نظرا للطبيعة الخاصة للمعلوماتية عبر الانترنت يراه الآخر ممنوع فيجرم، ومرد ذلك إلى طبيعة النظام القانوني السائد في كل بلد من البلدان.[1]

وبالرغم مما أصدرته البلدان الأوربية من تشريعات تكافح الجريمة المعلوماتية إلا أنها ليست جامعة مانعة، بدليل أن مؤسساتها المحلية تطالب في كل عام بإضافة نماذج من السلوك الإجرامي المعلوماتي لتكون محلا للتجريم.

2 ــ صعوبة التنسيق المحكم فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة الإلكترونية بين الدول خاصة فيما يتعلق بأعمال الاستدلال والتحقيق في مثل هذه الجرائم خارج نطاق حدود الدولة فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته.

3 ــ ثبوت قصور في المعاهدات والاتفاقات الثنائية والدولية لعدم تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الانترنت، ومن ثم تطور الجريمة المعلوماتية بذات السرعة

---

(1) الإحالات في النسخه المطبوعه.

(2) الإحالات في النسخة المطبوعة.

...../...

على نحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول، وبذلك يبرز الأثر السلبي في التعاون الدولي.

4 ـــ كما تعد الجرائم الإلكترونية من أكثر الجرائم إثارة لمسألة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع جريمة إلكترونية في مكان معين، وتنتج آثارها في مقاطعة أخرى داخل الدولة أو خارجها، ومن هنا تنشأ مشكلة البحث عن الأدلة الجنائية على شبكة الانترنت خارج دائرة الاختصاص التي قدم فيها البلاغ أو تم تحريك الدعوى الجنائية فيها، ومن أبرز المشاكل التي تظهر في هذا المجال ما يتعلق بفحص البيانات في مراكز معلومات دول أخرى وهو ما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدول باعتبار السيادة الوطنية التي قد لا تسمح في كثير من الأحيان بهذا النوع من التحقيقات نظرا للحساسيات الدولية المعروفة حاليا سواء في المجالات السياسية أو غيرها، كما قد يؤدي بطء الإجراءات الرسمية إلى فقدان الأدلة، وقد تكون بلدان متعددة متورطة في الأمر، وهو ما يشكل تحديا كبيرا لمتابعة وحفظ الأدلة.

كما تعد المساعدة الرسمية المتبادلة بين البلدان في هذا المجال من العمليات الأكثر إرهاقا التي يتم اللجوء إليها عادة عملا بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية، حيث يشترط في الغالب أن تكون الجريمة المعنية على درجة معينة من الخطورة وأن تشكل جريمة معترف بها في كل من البلدان الطالبة والموجهة إليها الطلب، أي وجوب اعتبارها بما يسمى "التجريم المزدوج".[1]

ولذلك فإن دور القانون لا يتوقف على مجرد تنظيم العلاقات المترتبة على التقدم التكنولوجي بل يجب أن يحمي القيم التي تحيط باستخدام التكنولوجيا، ويحدد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي حتى لا يتخذه المجرمون أداة لتطوير وسائل إجرامهم وهو ما لا يمكن تحقيقه إلا من خلال تشريع رباني.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخه المطبوعه.

...../...

الباب الرابع

المسؤولية الجنائية عن الجرائم الإلكترونية في التشريع الجنائي الإسلامي

الفصل الأول: جرائم الأعتداء على المال وحكمها في الفقه الجنائي الإسلامي.

الفصل الثاني: جرائم الأعتداء على النفس والعرض وحكمها في الفقه الجنائي الإسلامي.

الفصل الثالث: جرائم الأعتداء على أمن الدولة والمجتمع وحكمها في الفقه الجنائي الإسلامي

1)
2)
..

تمهيد:

لقد تضمنت الشريعة الإسلامية أصولا وقواعد صالحة لمواجهة كل أوضاع الحياة وظروف الزمان والمكان، كقاعدة " لا ضرر ولا ضرار"، وقاعدة "سد الذرائع"، وقاعدة "دفع المفاسد مقدم على جلب المصالح"، كما خولت لولي الأمر تقرير العقوبات في بعض أنواع الجرائم مراعاة منها للمصلحة العامة للمجتمع، ونصّت على عقوبات ثابتة لا تتأثر باختلاف الأوضاع والظروف، وبذلك جمعت في التجريم والعقاب بين الثابت والمرن والأصالة.

وإن مرونة الشريعة الإسلامية يجعلها صالحة لكل زمان ومكان ولكل ما هو مستحدث من أفعال وتصرفات لم تعهد من قبل وذلك باعتبار أن كل فعل يخالف أوامر الدين الإسلامي يعاقب عليه[1]، وهو الإطار العام للأفعال المقبولة وغير المقبولة حديثها وقديمها. وعلى هذا فإن قضية الجريمة والعقوبة ونوازلها أمر محسوم في الفقه الجنائي الإسلامي لكونه يتسم بوضع متميز بين سائر التقنيات الجنائية المقارنة؛ فالتجريم والعقاب في النظام الإسلامي يتوجه مباشرة إلى صيانة وحماية المصالح المعتبرة في الإسلام والممثلة في الدين والنسل والنفس والمال والعقل، وأي اعتداء على هذه المصالح يعد جريمة يعاقب فاعلها، وهو سر تفوق الشريعة الإسلامية على القوانين الوضعية.

وعلى ضوء ذلك سأبين في هذا الباب التطبيقي أهم أنواع الجرائم الإلكترونية التي صنفتها وفق ما تلحقه من أضرار بالمصالح المعتبرة في الإسلام، وسأعالجها من وجهة النظر الشرعية وذلك في الفصول التالية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الأول:
جرائم الاعتداء على المال وحكمها في الفقه الجنائي الإسلامي

المبحث الأول: جرائم التعدي على الحاسوب والبرامج.

المبحث الثاني: جرائم التعدي على المواقع الإلكترونية.

المبحث الثالث: جرائم التزوير الإلكتروني.

المبحث الرابع: جرائم التعدي على النقود الإلكترونية.

المبحث الخامس: جرائم التعدي على التجارة الإلكترونية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: جرائم التعدي على الحاسوب والبرامج[1]

من الصعب الإلمام بكل استخدامات الحاسوب وتطبيقاته في مناحي الحياة المختلفة لأنه أصبح جزءا لا يتجزأ من ممارسات وحياة الإنسان اليومية، كما عرف الحاسوب في مجال الجرائم الإلكترونية أدوار مختلفة؛ فمن وسيلة لاكتشاف الجريمة إلى أداة للإجرام الإلكتروني وقد يكون أيضا ضحية للجريمة وذلك لما يتعرض له من اختراقات وتدمير لمعطياته، أوسرقة ملفاته أو تعديلها، أو المساس بالمعلومات المحفوظة بداخله كملفات الحالات الجنائية أو المعلومات العسكرية وخطط التسويق والتصنيع، أو سرقة الأسرار التجارية، أو تعطيل كفاءة أنظمته عن طريق نشر الفيروسات وغيرها من الجرائم، ولذلك يكاد الحاسوب أن يكون العنصر الأساسي الأول المستهدف في الجرائم الإلكترونية.

المطلب الأول: جريمة التعدي على معلومات الحاسوب

إن سرقة الحاسوب ككيان مادي لا يثير مشكلة بالنسبة لمادية المال محل السرقة لأن هذا الفعل سيخضع لنصوص السرقة، ولكن الإشكال يحصل عندما يقوم الجاني بالاعتداء على المكونات المعنوية للحاسوب من معلومات وبرامج ونظم.. فهل يمكن تصور قيام جريمة السرقة في حال الاستيلاء على مكوناته التي تفتقد إلى الأثر المادي؛ كالدخول غير المسموح به إلى الحاسوب والاطلاع على المعلومات المخزنة بوسائطه، لأن ما يعرف عن السرقة أن الشيء المسروق ينتقل من حيازة المالك إلى حيازة السارق، أما المعلومات فقد يسرق الجاني نسخة منها بينما يبقى أصلها في حيازة صاحبها وهو ما جعل بعض الباحثين يرون أن البرامج والمعلومات لا تعتبر محلا للسرقة[2]، وهو تصريح من شأنه تجريد المعلومات والبرامج والنظم من الحماية الجنائية، لكن لو قمنا بقياس سرقة المعلومة على سرقة التيار الكهربائي أو خدمات الهاتف باعتبارها من قبيل الأشياء التي يمكن السيطرة عليها وضبطها

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وتقييمها[1]؛ فإذا كانت الكهرباء عبارة عن قوة وطاقة تخضع لسيطرة من يقوم بتوليدها والاستحواذ عليها وتمكين غيره من الاستفادة منها وفقا للضوابط والشروط التي يضعها وهو ما يجعلها صالحة للحيازة والملكية، فإن المعلومات كذلك تخضع لسيطرة من يبتكرها أو يقوم بمعالجتها آليا، كما تخضع لموزعها أو منتجها وأصبح لها مقابل مادي وهو ما يصبغها صفة الأموال المتقومة التي تصلح للتداول، ولذلك كسبت المعلومات صفة المالية بغض النظر عن الخلاف الفقهي حول طبيعة هذا المال، هل هو من الأموال المثلية أو القيمية؟ فما يمكن جزمه أنها أموال معنوية ينتج عنها بالضرورة آثار مادية ملموسة[2].

ولإثبات ذلك من الوجهة الفقهية فلابد من مقارنة طبيعة المعلومات التي يحتويها الحاسوب بخصائص المال لاستنتاج نسبة التطابق التي ذكرتها وذلك كما يلي:

الفرع الأول: خصائص المال في الفقه الإسلامي

يعرّف المال في اللغة؛ كل ما يقتنى ويحوزه الإنسان بالفعل سواء أكان عينا أم منفعة، كذهب أو فضة أو حيوان أو نبات أو منافع الشيء كالركوب والملبس والسكنى، أما ما لا يحوزه الإنسان فلا يسمى مالا في اللغة كالطير في الهواء والسمك في الماء والمعادن في باطن الأرض[3].

ويعرّف المال في الاصطلاح الفقهي على رأيين:

أولا ـــ عند الحنفية: المال هو كل ما يمكن حيازته وإحرازه وينتفع به عادة، فالمالية عندهم تتطلب عنصرين؛ الأول إمكانية الحيازة والإحراز حيث لا يعد مالاً ما لا يمكن حيازته كالأمور المعنوية مثل العلم والصحة والشرف والذكاء، وما لا يمكن السيطرة عليه كالهواء الطلق وحرارة الشمس وضوء القمر. والعنصر الثاني الذي تتطلبه المالية عند الحنفية عادة الانتفاع، فكل ما لا يمكن الانتفاع به أصلا كلحم الميتة، والطعام المسموم، أو الفاسد، أو ينتفع به انتفاعا لا يعتد به عادة عند الناس كقطرة ماء أو حفنة تراب فلا يعد مالا، لأن العادة تتطلب الاستمرار بالانتفاع بالشيء في الظروف العادية، كما لا يعد مالا ما ينتفع به عند الضرورة كلحم الميتة عند الجوع الشديد لأن ذلك

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ظرف استثنائي[1].

ثانيا ـــ ويعرّف المال عند جمهور الفقهاء دون الحنفية: هو كل ما له قيمة يلزم متلفه بضمانه[2].

فالحنفية حصروا معنى المال في الأشياء والأعيان المادية المحسوسة، أما المنافع والحقوق فليست أموالا عندهم وإنما هي ملك لا مال، بينما اعتبرها غيرهم من الفقهاء أموالا؛ لأن المقصود من الأشياء منافعها لا ذواتها، وهو الرأي الراجح المعمول به في الفقه وعرف الناس ومعاملاتهم، كما يجري عليها الإحراز والحيازة[3].

وقد قال في ذلك جمهور الفقهاء أن المنافع تعتبر مالا لإمكان حيازتها بحيازة أصلها ومصدرها، ولأنها هي المقصودة من الأعيان، ولولاها ما طلبت ولا رغب الناس بها[4]، وبناء على ذلك من غصب شيئا وانتفع به مدة ثم رده إلى صاحبه فإنه يضمن قيمة المنفعة عند غير الحنفية، وهو ما يجعل الحقوق المالية تتعلق بالأموال والمنافع، ومن خلال هذه التعريفات يمكن استخلاص الخصائص التالية:

ـــ أن المال ما يميل إليه طبع الإنسان، ويمكن إحرازه سواء كان عينا أو منفعة.

ـــ أن المال يكون مما يبذل ويحمى من الاعتداء عليه[5].

ـــ أن المال يتحقق الانتفاع به في حال الاختيار دون الضرورة.

ولو قمنا بإسقاط التعريف الاصطلاحي للمال وخصائصه على المعلومات الإلكترونية فإنه يمكن القول بأن المعلومات هي من الأموال المتقومة باعتبارها منفعة مالية يجوز التعامل بها في عقود المعاوضات [6] .

الفرع الثاني: المسؤولية الجنائية في التعدي على معلومات الحاسوب

يعرف الركن المادي في جريمة السرقة بفعل الاختلاس والذي يتكون من عنصرين موضوعي وشخصي؛ أما العنصر الموضوعي فيتمثل في التصرف الإرادي الذي يؤدي إلى نتيجة، إذ هناك سلوك

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ونتيجة ورابطة سببية بينهما، والعنصر الشخصي يتمثل في نية المجرم في الاستحواذ على الشيء أو تملكه وفقا للتعبير التقليدي ومن جانب آخر عدم الرضا الصادر من المجني عليه لاستيلاء الجاني على ماله.

ولو نطبق هذه المبادئ العامة على سرقة المعلومات فإنه يتحقق النشاط المادي الصادر من الجاني سواء عن طريق تشغيل الحاسوب للحصول على المعلومات، أو اختراقه له بأي وسيلة أخرى لتحقيق مقصده وهو ما ينشئ رابطة السببية بين النشاط المادي والنتيجة الإجرامية.

وبالنسبة للركن المعنوي الذي يقوم على أساس التكليف فإنه يتحقق بمسؤولية الجاني المرتبطة بالقصد الجنائي وهو الذي يعبر عنه بنية التملك مما يكشف عن نية الجاني في حيازة المعلومات، فنية التملك التي تتجه إليها إرادة الجاني هي عنصر آخر يضاف إلى عنصري العلم والإرادة في القصد الجنائي، وصورة ذلك أن الجاني يلجأ إلى التعدي على الحاسوب من أجل الاستحواذ على المعلومات وتملكها وهو يعلم أنها ملكا للغير، وبناء على ذلك يُطرح السؤال: هل يعد هذا الفعل سرقة موجبة للحد؟ وللإجابة عن ذلك لابد من تعريف السرقة وشروطها في الفقه الإسلامي لمعرفة مدى تحققها في هذا النوع من الجرائم.

الفرع الثالث: مفهوم السرقة في اللغة والاصطلاح

تعتبر السرقة من جرائم الحدود التي نهت عنها الشريعة الإسلامية صراحة لما يحصل منها من اعتداء على حقوق الآخرين وأخذ أموالهم بالباطل، وقد دلَّ على تحريمها الكتاب والسنة والإجماع، فقال تعالى:﴿وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَٰلًا مِّنَ ٱللَّهِۗ وَٱللَّهُ عَزِيزٌ حَكِيمٌ ﴾ [1]، وقال ﷺ: (لا يزني الزاني حين يزني وهو مؤمن، ولا يشرب الخمر حين يشربها وهو مؤمن، ولا يسرق السارق حين يسرق وهو مؤمن)[2].

أولا ــ تعريف السرقة في اللغة:

السرقة في اللغة: هي أخذ الشيء من الغير خفية، يقال: سُرق منه الشيء يُسرق سَرقاً وسَرَقة،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

واسترَقهُ، جاء إلى حرز مستترا فأخذ مالا لغيره، والاسم السرْقة[1].

ثانيا ــ التعريف الاصطلاحي للسرقة:

اتفق الفقهاء على اختلاف مذاهبهم على أن السرقة بالمعنى الشرعي يُطابق معناها المعنى اللغوي، لأن ركن السرقة بالمعنى الفقهي هو أخذ الشيء من الغير خفية، لكنهم اختلفوا في القيود الشرعية التي تعدُّ شروطا لترتب العقوبة عليها.

فعرّف الحنفية السرقة بأنها: أخذ الشيء من الغير خفية بغير حق نصابا كان أم لا، وأما باعتبار القطع فيه اشترطوا: أخذ مكلف ناطق بصير عشرة دراهم جياد أو مقدارها مقصودة ظاهرة الإخراج خفية من صاحب يد صحيحة مما لا يتسارع إليه الفساد في دار العدل من حرز لا شبهة ولا تأويل فيه[2].

وعرّفها المالكية فقالوا: هي أخذ مكلف نصابا من مال محترم لغيره بلا شبهة قويت خُفية، بإخراجه من حرزٍ غير مأذون فيه[3].

وعرّفها الشافعية: على أنها أخذ المال خفية ظلما من حرز مثله بشروط في السارق والمسروق منه[4].

وقال الحنابلة هي: أخذ مالٍ محترم وإخراجه من حرز مثله لا شبهة له فيه على وجه الاختفاء[5].

الفرع الرابع: شروط حد السرقة ومدى تحققها في سرقة المعلومات

من خلال التعريفات الاصطلاحية يمكن استخلاص شروط جريمة السرقة التي يثبت فيها حد القطع كما يلي:

1 ــ أن يكون الآخذ مكلفا.

2 ــ أن يكون المأخوذ مالا للغير.

3 ــ أن يبلغ النصاب (على خلاف).

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

4 ـــ أن يؤخذ من الحرز.

5 ـــ أن يؤخذ على سبيل الخفية والاستتار.

6 ـــ أن تنتفي عنه الشبهة.

وبإسقاط هذه الشروط على سرقة المعلومات فإن التكليف والأخذ من الغير متحقق فيها، وفيما يخص بلوغ النصاب الذي مقداره محل خلاف بين الفقهاء فإن تحديده هو من صلاحيات ولي الأمر الذي يعتمد في ذلك إلى مقتضيات الزمان والمكان حيث يكمن جوهره في أن يكون الشيء المسروق ذو قيمة يلحق الناس ضررا بفقدانه لأنه من عادة الناس التسامح في الأشياء البخسة، وفيما يخص هتك الحرز الذي هو محل خلاف أيضا بين الفقهاء في تحديد معناه حيث تعددت عباراتهم في المراد منه إلا أن حقيقته واحدة هي الحفظ والصون من التعدي اتفاقا، وفي ذلك عرّفه الموصلي من الحنفية بأنه: "ما يصير به المال محرزا عن أيدي اللصوص"[1]، وعرّفه المالكية بأنه: "ما من شأنه أن تحفظ به الأموال، كي يعسر أخذها مثل الأغلاق"[2]، وعرّفه الشافعية بأنه "ما يصير به المال محفوظا"[3]، وعرّفه الحنابلة بأنه "ما العادة حفظ المال فيه، ويختلف باختلاف الأموال والبلدان، وعدل السلطان وجوره، وقوته وضعفه"[4].

ويعود سبب عدم تحديد الحقيقة الاصطلاحية للحرز كونه يتغير بحسب الأمكنة والأزمنة والأعراف، لأن مقتضى قاعدة الأسماء المطلقة في الشريعة هو اعتبار الحقيقة الشرعية فإن لم توجد فاللغوية وإلا فالعرفية[5]، وقد نص جمهور الفقهاء على أن كل اسم ليس له حد في اللغة أو الشرع فالمرجع فيه للعرف[6] وهو ما يثير التساؤل حول مدى تحقق لفظ التعدي بالسرقة على الحاسوب باعتباره حرزا؟ وهل يعد الدخول إلى الحاسوب بطريق غير مأذون فيه انتهاكا لهذا الحرز فيستوجب حد السرقة؟

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

إن النظر إلى الحاسوب من حيث طبيعة معلوماته المالية وأهميتها لدى الصالح العام والخاص يجعل من الضرورة التحري في الطرق والوسائل التي تحفظه من التعدي، وقد اتخذت احتياطات جادة ومكلفة في هذا الجانب لضمان عدم التعدي كما سبق دراسته في الباب الثالث من البحث، وكل ذلك منعا من الحصول أو الاطلاع على الخصوصيات المالية والشخصية التي يحتوي عليها الحاسوب وهو ما يؤكد اعتباره حرزا يعاقب على التعدي عليه.

أما شرط الخفية والاستتار الموجب للحد في السرقة فهو غير متحقق في معظم جرائم الحاسوب لأن هذه الأخيرة يغلب عليها السرقة بالأخذ على سبيل الغصب والاختلاس والخيانة[1]، ولذلك يسقط حد السرقة لسقوط أحد شروطها الشرعية الذي يستوجب توفر ركن الخفية في أخذ المال نظرا لكون الاختلاس يقوم على المجاهرة، وفي ذلك ذهب جمهور الفقهاء إلى أنه لا قطع على المختلس استئناسا بقول النبي ﷺ: (ليس على خائن ولا منتهب ولا مختلس قطع)[2]، أما إذا ثبت شرط الخفية والاستتار كسرقة المال من الأجهزة الإلكترونية التي تعمل حتى أثناء غياب مستخدميها فإن المجرم يكون جزاؤه حد السرقة.

وفيما يخص شرط انتفاء الشبهة الذي يعني إلزامية كون المال المسروق مملوكا للغير، فإن كان في الملك شبهة فهو محل اختلاف الفقهاء، ومدار الخلاف عندهم أن يكون للشخص شبهة الملك في المال المسروق فإن اقترن بهذه الشبهة ولو ضعيفة لا يقطع على أساس أن المالك لا يسرق مال نفسه أو جزء من مال نفسه[3]، كما تقع أيضا شبهة الدليل في السرقة؛ كسرقة بيت المال، أو سرقة المدين، أو سرقة الإعارة، أو سرقة الأقارب[4]، ومن ثم فإن المعتدي على المعلومات في الحاسوب إن كان أحد هؤلاء لا تنطبق عليه عقوبة الحد لقيام الشبهة في دليل السرقة، ويطبق عليه الحد إن ثبت أن المال مملوك للغير، وفيما يخص الحالات التي لا يطبق فيها الحد لا يعني ذلك عدم إيقاع العقوبة التعزيرية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المناسبة للفاعل والتي يحددها ولي الأمر بحسب دواعي المصلحة وذلك اعتبارا بأن الفاعل تعدى على حق الله أو حق الآدمي أو عليهما معا[1].

والنتيجة أنه رغم الاتفاق الحاصل في عناصر جريمة السرقة الواقعة على الحاسوب مع الجريمة التقليدية إلا أنها تختلف عنها فيما يخص احتمال قيام الشبهة في المال المسروق، هذا بالإضافة إلى إشكالية عدم تبليغ أو مطالبة معظم الضحايا بما سرق منهم في غالب الأحيان ويعود السبب في ذلك إلى عدة عوامل أهمها الخوف من المساس بسمعة الضحية ـــ خاصة الأشخاص المعنويين ـــ أو غلبة الظن بعدم استرداد الحق لكون الجريمة الإلكترونية عابرة للحدود خاصة إن كان الجاني خارج إقليم المجني عليه[2]، لكن يبقى القول بأن سرقة المعلومات يمثل غصبا لمال معنوي متقوم يحرم التعدي عليه ويستوجب إما الحد أو التعزير شرعا، وقد نهانا الله عز وجل من أكل المال بدون وجه حق في قوله تعالى:﴿ وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ ﴾ [3].

المطلب الثاني: جريمة التعدي على برامج الحاسوب

تشكل البرامج الكيان المعنوي أو المنطقي لنظام الحاسوب، فبدونها لا تكون ثمة فائدة لمكوناته المادية وقد ورد في شأنها تعريفات عديدة كما سبق ذكره من بينها "هي مجموعة التعليمات التي تسمح بعد نقلها على دعامة تستطيع الآلية قراءتها لبيان أو أداء أو إنجاز مهمة أو وظيفة أو نتيجة معينة بواسطة آلة لمعالجة المعلومات"[4] ، وتعرف أيضا بأنها "مجموعة العبارات أو التعليمات التي تستعمل مباشرة في الحاسب الآلي لغرض إظهار نتيجة محددة"[5]، وتنقسم البرامج من الناحية التقنية إلى نوعين: برامج التشغيل وهي المسؤولة على عمل مكونات النظام وتعرف بالبرامج النظامية كما تعمل أيضا على توفير بيئة مناسبة لعمل النوع الثاني من البرامج وهي البرامج التطبيقية بحيث إذا حصل

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أي خلل بالبرامج النظامية فإنه يؤثر سلبا على عمل البرامج التطبيقية، وهذه الأخيرة أنواعها متعددة ومختلفة باختلاف مهامها كمعالجة النصوص، ومعالجة الجداول، ومعالجة الرسوم، والمحاسبة، والمعالجة السمعية البصرية وغيرها [1].

وتنقسم البرامج من ناحية الحماية إلى برامج محمية وأخرى غير محمية، وتعتبر المحمية منها من أغلب البرامج استخداما حيث لا يسمح بتعديلها أو نسخها أو إعادة توزيعها إلا بالرجوع إلى مصدرها الأصلي، كما تنقسم الحماية فيها على نوعين: حماية فنية كتشفير البرنامج بمفتاح أو وصلة لا يعمل بدونها، والنوع الثاني الحماية النظامية حيث يظهر مصدّر البرنامج كتابات تفيد أن هذا المنتج محفوظ الحقوق، أما البرامج غير المحمية فهي البرامج التي لا يمنع أصحابها من نسخها والاستفادة منها وتوزيعها ومن أمثلتها؛ ما يعرف بالبرامج الحرة وهي تهدف عادة إلى التقليل من ضغوط الشركات المنافسة ومثالها ما قامت به الصين حيث أتاحت النسخة الكاملة لبرنامج لينكس UNIX النظامي مجانا بغرض تشجيع استخدامه بدلاً من نوافذ مايكروسوفت WINDOWS ، وبذلك خففت من ضغوط المنافسة الأمريكية عليها في هذا المجال، ورغم أن البرامج الحرة تمنح حقوق استعمالها إلى الغير مجانا فإن ذلك لا يعني أنها ملكا عاما أو خارج نطاق الملكية الفكرية، بل تبقى خاضعة للشروط التي يحددها المنتج ـــ مصمم البرنامج ـــ.

أما عن فوائد البرامج المعلوماتية تجاه المجتمع، فإن دورها لا يستهان به في تحسين الاقتصاد وتطوره، وتيسير المعاملات الحكومية والتجارية والمصرفية خاصة البنكية منها، بالإضافة إلى دورها في تطوير وسائل الاتصال والنهوض بالتقدم العلمي، وتيسير إدارة المؤسسات العامة والخاصة وغير ذلك من الفوائد التي تعود على الصالح العالم بالنفع والتيسير[2].

ولقد لقيت طبيعة برامج الحاسوب وموضع حمايتها جدلا واسعا تبنته مدرستان؛ فذهبت الأولى إلى اعتبار برامج الحاسوب ذات صبغة صناعية مما يستوجب حمايتها في إطار قوانين براءة الاختراع، في حين ذهبت المدرسة الثانية إلى أن برامج الحاسوب ما هي إلا أفكار وترتيبات لخوارزميات تفرغ في شكل إبداعي وبالتالي فإن حمايتها تكون ضمن حماية حقوق الملكية الفكرية، وفي هذا المجال أيضا

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

يرى البعض أن هذه البرامج ما هي إلا سر من الأسرار التجارية مما يستوجب حمايتها وفق نظم الأسرار التجارية، و يرى البعض الآخر وجوب حماية هذه البرامج وفق الشروط العقدية المفروضة في اتفاقيات الاستخدام[1].

وبالرغم من هذا الاختلاف النظري، فقد سارعت غالبية التشريعات والاتفاقيات الإقليمية[2] والدولية[3] إلى حسم الأمر، حيث أدرجت برامج الحاسوب ضمن لائحة الأعمال الأدبية Literary Work وأُخضعت لحق المؤلف، وهو ما أحاطها بالحماية القانونية كمصنف أدبي سواء أكانت على مستوى مصدر الصياغة "الشفرة" Source Code أو على مستوى موضوع هدف الصياغة Object Code وبغض النظر عن الوسيط الحامل لها[4]، وذلك سعيا إلى الإحالة دون تفاقم ظاهرة القرصنة لبرامج الحاسوب كالنسخ غير المشروع أو الاستخدام غير المرخص به للبرامج والتي كبدت الصناعات المعلوماتية والشركات العاملة في هذا المجال خسائر جمة[5].

الفرع الأول: مفهوم نسخ البرامج وصوره

نسخ البرامج هو عملية استنساخ برنامج أصلي بأي وسيلة كانت من طرف شخص طبيعي أو معنوي دون استصدار إذن من المالك، ويتخذ نسخ البرامج صورا عديدة أهما:

ـــ نسخ البرنامج الأصلي المرخص للعمل على جهاز رئيسي، وتثبيت تطبيقه في مجموعة من الأجهزة للاستفادة من خدماته عن طريق التحايـــل الإلكتروني باستعمـــال الشبكة المحلية Intranet

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الموصولة بالجهاز الرئيسي[1] بدل شراء مجموعة من البرامج المشفرة بعدد الأجهزة المستعملة.

ـــ نسخ برنامج بدون إذن المالك ورفعه على شبكة الانترنت سواء بهدف العرض المجاني، أو تسويقه عبر المواقع المنتشرة على الشبكة والمتخصصة في بيع البرامج المقرصنة.

ـــ تفكيك شفرة حماية البرامج الأصلية المتوفرة على شبكة الانترنت، ومن ثم نسخها وبيعها بغرض الحصول على المال، أو بغرض النشر المجاني مما يلحق الضرر بمنتجي البرامج.

ـــ تفكيك شفرة حماية البرامج التجريبية الموجهة للجمهور، وذلك عن طريق إزالة الحماية أو تعطيلها مما يجعل هذه البرامج متاحة للجميع ويتم نسخها وبيعها أو نشرها وهو ما يلحق أضرارا جسيمة بحقوق مؤلفيها ومصمميها.

ـــ النسخ المكثف للبرامج الأصلية على الأقراص باستعمال أجهزة الاستنساخ الإلكترونية بدون ترخيص مصدرها الأصلي والمتاجرة بها، وقد عرف هذا النوع من التجارة الممنوعة رواجا كبيرا في الكثير من الدول سواء العربية منها أو الأجنبية نظرا للإقبال الكبير عليها باعتبار أسعارها المنخفضة، ففي الجزائر مثلا نشر تحقيق على الانترنت يشير أن نسبة القرصنة لبرامج الكومبيوتر والألعاب الإلكترونية بلغ 85 بالمائة بحسب الإحصاءات الرسمية سنة 2011 ، وهو معدل يبين مدى درجة الانتهاكات الخطيرة التي تتعرض لها حقوق الملكية الفكرية لأصحاب هذه البرامج من المؤسسات العالمية، ومن جانب آخر يشير هذا المعدل إلى الحجم الكبير لعملية استغلال الأقراص المنسوخة بطرق غير مشروعة وهو أمر ليس حكرا فقط على الأفراد بل تمتد استعمالاته لإدارات ومؤسسات رسمية[2]، وجاء في دراسة أخرى حول موضوع القرصنة أن نسبة 57 بالمائة من مستعملي الحاسوب في الجزائر صرحوا باكتسابهم برامج معلوماتية غير أصلية[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني: مشروعية حق ابتكار البرامج

لقد عرفت برامج الحاسوب جدلا واسعا فيما يخص حمايتها ضمن قانون براءة الاختراع أو الملكية الفكرية أو حمايتها ضمن قانون الأسرار التجارية، وتم الإجماع على إدراجها ضمن حق التأليف كما سبق ذكره، وإنّ تفحص هذا الجدل يثبت أن هناك إجماع عام بأن برامج الحاسوب النافعة هي من الأموال المتقومة التي تستوجب الحماية ويمنع التعدي عليها ومن أجل ذلك تم إدراجها ضمن حق التأليف، فما مفهوم حق التأليف وما مدى مشروعيته؟

أولا ــ تعريف الحق لغة واصطلاحا:

1 ــ الحق في اللغة نقيض الباطل، يقال، حق الشيء يحق: إذا ثبت ووجب، ويطلق على المال والملك والأمر الثابت الموجود، والحزم[1].

2 ــ والحق في الاصطلاح الفقهي: يستعمل في مقابلة الأعيان والمنافع المملوكة، ويريدون به ما يثبت للأشخاص من مصالح بالاعتبار الشرعي، دون أن يكون لها وجود إلا بهذا الاعتبار؛ كالطلاق والحضانة[2].

ويعرّف الحق أيضا في الاصطلاح بأنه: اختصاص يقرر به الشرع سلطة أو تكليفاً[3].

وهو تعريف يشمل أنواع الحقوق الدينية كحق الله تعالى على عباده من صلاة وصيام ونحوهما ، ويشمل أيضاً الحقوق المدنية كحق التملك والحقوق الأدبية، والحقوق العامة، والحقوق المالية وغيرها.

أما الحق الشخصي، فهو ما يقره الشرع لشخص على آخر، ومحله إما أن يكون قياماً بعمل، وإما أن يكون امتناعاً عن عمل ، وللحق الشخصي ثلاثة عناصر هي : صاحب الحق ، ومحل الحق ، والمكلف، كما يقصد أيضا بالحق الشخصي حماية مصلحة الشخص، سواء كان الحق عاما كالحفاظ على الصحة والأموال وتحقيق الأمن، أم كان الحق خاصا كرعاية حق المالك في ملكه وحق الشخص في بدل ماله المتلف[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثانيا ــ تعريف التأليف في اللغة والاصطلاح:

1 ــ التأليف لغة: هو انضمام الشيء بالشيء وهو ضم الأشياء الكثيرة؛ ليطلق عليها اسم واحد.[1]

2 ــ ويعرّف التأليف اصطلاحا بأنه: الكلام المدون الذي ينطوي على عمل إبداعي، أيا كانت درجة أهميته[2].

ثالثا ــ مشروعية حق التأليف:

نظرا لعدم توفر نص صريح أو حكم مسبق في مسألة حق التأليف كونه من القضايا المستجدة فقد عرف اختلافا لدى الفقهاء المعاصرين بين اعتبار حق المؤلف وعدمه على قولان:

القول الأول: عدم اعتبار حق المؤلف، وبالتالي يحرم فيه المقابل المالي، ولا يجرم بالاعتداء عليه.[3]

وقد استدل أصحاب هذا القول في حكمهم من الكتاب، والسنة، والقياس، والمعقول:

ــ فمن الكتاب قوله تعالى:﴿ إِنَّ ٱلَّذِينَ يَكۡتُمُونَ مَآ أَنزَلۡنَا مِنَ ٱلۡبَيِّنَٰتِ وَٱلۡهُدَىٰ مِنۢ بَعۡدِ مَا بَيَّنَّٰهُ لِلنَّاسِ فِي ٱلۡكِتَٰبِ أُوْلَٰٓئِكَ يَلۡعَنُهُمُ ٱللَّهُ وَيَلۡعَنُهُمُ ٱللَّٰعِنُونَ ﴾ [4].

ووجه الدلالة: أن الله عز وجل توعد باللعنة من يكتم العلم، ولذلك فإن إيجاب حق المؤلف وإعطاؤه الحق في النشر أو المنع فيه كتم للعلم، وعليه يستحق اللعن بمنطوق الآية، واللعنة لا تكون إلا على حرام، وكذا فإن القول بحق التأليف حرام شرعا.

ــ ومن السنة النبوية، قوله ﷺ: (ما من رجل يحفظ علما فيكتمه، إلا أتى به يوم القيامة ملجما من النار)[5].

ووجه الدلالة: إن إعطاء المؤلف الحق في النشر والمنع فيه كتم للعلم وعليه فقد توعده الله بعقاب أليم بأن يلجم بلجام من النار كما لجم علمه على الناس، والوعيد بالنار يفيد التحريم.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ ومن القياس: يقاس حق التأليف على حق الشفعة؛ من حيث كونه حقا مجردا، فلا يجوز الاعتياض عنه.

ـــ أما من المعقول: فقالوا أن العلم يعتبر قربة وطاعة، والقربة لا يجوز فيها الحصول على أجر مالي في أدائها[1].

ومن باب مقاصد الشريعة، أن تقديم المصلحة العامة على الخاصة والحفاظ عليها هي عين المصلحة، بحيث لو تعارضت مصلحة الفرد مع الجماعة فلا اعتبار لها لأنه ليس من العدل إهمال المصلحة العامة من أجل المصلحة الخاصة وإلا ترتب على ذلك الفساد، ومن هنا كانت الحقوق ليست تبعا للهوى والشهوة، فإيجاب حق المؤلف هو تحقيق لمصلحة المؤلف بغض النظر عن الجماعة وهذا باطل[2].

القول الثاني: وهم القائلون بحق التأليف حيث يجيزون العائد المادي ويحرمون المعتدين عليه، وأصحاب هذا القول هم: مصطفى الزرقا، والدريني، والبوطي، والزحيلي[3]، وقد استدلوا في ذلك من الكتاب والسنة، والمعقول، والعرف، والمقاصد، والمصالح المرسلة كما يلي:

ـــ من بين أدلتهم من القرآن الكريم قوله تعالى:﴿ وَلَا تَبۡخَسُواْ ٱلنَّاسَ أَشۡيَآءَهُمۡ ﴾[4].

ووجه الدلالة: أن الآية تنهى عن انتقاص حقوق الناس، فالواجب أن يوفى الناس حقهم ماديا أو معنويا؛ وعليه فلا يجوز انتقاص حق المؤلف جزءا أو كلا.

وأيضا قوله تعالى:﴿ وَأَن لَّيۡسَ لِلۡإِنسَٰنِ إِلَّا مَا سَعَىٰ ۝٣٩ وَأَنَّ سَعۡيَهُۥ سَوۡفَ يُرَىٰ ﴾[5].

ووجه الدلالة: أن الإنسان لا يلزمه نيل الأجر في الآخرة الحرمان من حقه في الدنيا، وإلا أدى ذلك إلى حبس الحقوق واختلال نظام المعايش[6]، وحق التأليف واحد من هذه الحقوق.

ـــ ومن السنة الشريفة استدلوا بمجموعة من الأحاديث منها:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ عن النبي ﷺ أنه قال: (إذا مات ابن آدم انقطع عمله إلا من ثلاث؛ وذكر منها: علم ينتفع به...)[1].

ووجه الاستدلال أن الحديث يؤكد عدم انفصال الأثر العلمي عن صاحبه في نظر الشرع بدليل عدم بطلانه بعد وفاته، حيث يستمر تلقي الأجر عليه باستمرار نفعه وأثره[2].

ـــ وعن النبي ﷺ قال: (المسلمون على شروطهم)[3].

ووجه الاستدلال، أن الحديث يشير إلى أن الأصل في الشروط الحل ولذلك من الضروري التزام المسلمين بشروطهم وعهودهم، ومادام المؤلف يشترط عدم النسخ، أو الطباعة إلا بإذنه فيجب الوفاء بهذا الشرط.

ـــ وفي حديث آخر عن أبي حرة الرقاشي عن عمه، قال: قال رسول الله ﷺ :(لا يحل مال امرئ مسلم إلا بطيب من نفسه)[4].

ووجه الدلالة، أن الحديث يحرم الاعتداء على أموال الغير، فلا يحل ذلك إلا باستئذان صاحب المال، وكذا في حق المؤلف يلزم عدم الاعتداء على مؤلفه بالنسخ، أو الطباعة وغيرها إلا بإذن منه.

وما يدعم ذلك أن المنافع تعد أموالا متقومة عند جمهور الفقهاء غير الحنفية وهي من الحقوق المعنوية، فمادام الناتج الذهني يمثل منفعة من منافع الإنسان فهو مال يصح عنه المعاوضة شرعا[5].

كما استدلوا قياسا بحق الصانع في تملكه لما أنتجه أو صنعه بأن يتيحه للغير للاستفادة منه أو يمنع ذلك لأنه حبس نفسه وبذل الجهد والوقت والمال وهو ما ينطبق على الناتج الذهني، ودليلهم من القواعد الفقهية أن الإنسان محاسب على ما يصدر عنه من أقوال، وبناء على ذلك يكون له الحق فيما أبدعه عملا بقاعدة "الغرم بالغنم، والخراج بالضمان"[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما استندوا إلى مقاصد الشريعة باعتبار أن انتفاء الحق المالي للمؤلف يناقض مقتضى الأصل العام في التشريع من أن لكل إنسان حقه الكامل في ثمرة جهده المالي فلا يجوز هضمه لأنه ضرب من أكل أموال الناس بالباطل، وهو ما يحرم صراحة في النص الشرعي.

واستدلوا في إطار المصالح المرسلة، أن عدم اعتبار حق الملك والمالية لابتكار العالم سيفضي في الغالب إلى عزوف العلماء عن الاستمرار في الابتكار والإنتاج، وهو مآل ممنوع شرعا وينافي المصلحة فوجب أن تسد الذريعة إلى هذا المآل[1]، فعدم حماية هذه البرامج لأصحابها يجعلهم يحجمون عن الاستمرار في إنتاجها إما لخسارتهم أو لأنهم لم يجنوا إلا التعب، وبتوقفهم يحرم المجتمع من أسباب الرفاهية والسعادة والتيسير في أمور حياتهم، وهذا يعد إضرار بالمجتمع والرسول ﷺ يقول: (لا ضرر ولا ضرار)[2]، كما قال أيضا ﷺ : (من سبق إلى ما لم يسبق إليه مسلم فهو له)[3]، وهو حديث يتبين منه أن منتجي برامج الحاسوب أحق بإنتاجهم من غيرهم لأنهم سبقوا إليها فوجب حمايتها لهم.

وبالنظر لبرامج الحاسوب وما تتعرض له من قرصنة من قبل الباحثين عن الكسب السريع، نجد أن المصلحة متحققة في حمايتها من القرصنة وفرض عقوبات على المخالفين، باعتبار أن هذه المصلحة مصلحة جماعية وليست شخصية، وضرورية وليست تعسفية، ومعقولة وليست تسلطية.

واستدلوا من العرف، أن القيمة المالية في الشيء إنما يبرزها العرف الاجتماعي؛ فإقبال الناس على شيء ما لأجل الاستفادة منه أو الإعراض عنه هو الذي يكسب ذلك الشيء القيمة المالية من عدمها، وقد عرف الناس على المستوى العالمي إقبالا كبيرا في استعمال البرامج واقتناءها لما تدره من مصالح عامة وخاصة، كما نادت هيئات رسمية ودولية بوجوب الحماية باعتبار البرامج ذات حقوق مادية وهو ما يدعم الدليل العرفي[4].

وبناء على ذلك فإنه يرجح القول الثاني الذي أضم إليه رأيي، لأنه يثبت حق المؤلف ومنتج البرامج، وهذا يعود إلى قوة الأدلة التي جاؤوا بها وسلامتها من النقد السلبي، كما أن تحليلهم يخدم أهم مقصد من مقاصد الشريعة ألا وهو العقل للمؤلف والمتعلم على حد سواء؛ فالعمل بذلك يرتقي

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وينهض بالمجتمع بأسره كما أن حق المؤلف يعتبر أكثر ملامسة لفقه الواقع، فتشجيع عملية العلم والإبداع عن طريق ماليتها وحمايتها سيكفل استمرارية التأليف والإنتاج وعدم الجنوح إلى أنشطة أخرى قد تؤثر على عجلة العلم والإبداع، كما أن حق المؤلف أصبح معترف به في القوانين والأعراف مما يوجب التعويض عن الظلم والعدوان لأصحاب الحق، والمسلم أولى الناس برعاية الحقوق والوفاء بها.[1]

كما يؤيد ترجيح هذا القول ويقويه، القرار رقم 5 المتعلق بالحقوق المعنوية الصادر عن مجمع الفقه الإسلامي في دورته الخامسة المنعقدة في الكويت من 1 إلى 6 جمادى الأولى سنة 1409هـ وذلك في البند الأول والثالث والذي جاء فيه: " أن التأليف والاختراع والابتكار هي حقوق خاصة لأصحابها أصبح لها في العرف المعاصر قيمة مالية معتبرة لتمول الناس لها، وأنه يعتد بها وهي مصونة شرعا ولأصحابها حق التصرف فيها ولا يجوز الاعتداء عليها"[2].

الفرع الثالث: حكم التعدي على برامج الحاسوب

تقوم سياسة التجريم في الشريعة الإسلامية على ما تقوم عليه التشريعات الحديثة وهو فكرة الضرر بمعنى انتهاك المصالح والقيم التي يريد الشارع حمايتها وصيانتها ضد أي تعد عليها، وهذه المصالح والقيم المحمية في المجتمع الإسلامي هي ما يطلق عليها الفقهاء "مقاصد الشارع"، وقد حدد الإسلام هذه المقاصد بالضروريات والحاجيات والتحسينيات ومن الضروريات حفظ المال[3].

ومن المعلوم في الشريعة الإسلامية أن المصالح التي سكت عنها الشارع والمعروفة بالمصالح المرسلة وما يتصل بالتعازير، كل ذلك مما تترك للإمام تقديره أو منعه أو تقييد إباحته وفرض العقوبة على المخالفين تحقيقا للمصلحة العامة أو دفع الضرر عن المجتمع، ولأن حفظ برامج الحاسوب هو حفظ للمال باعتبارها مصلحة ضرورية، فإنه يحق للإمام شرعا إذا توافرت شروط المصلحة العامة أن يمنع استنساخ برامج الحاسوب والمتاجرة فيها بطرق غير مشروعة، لهذا كان منع التعدي على البرامج موافقا للشريعة الإسلامية[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وبناء على موقف الفقهاء وما اتفق عليه العلماء المعاصرين من ضرورة حفظ الحقوق، فإن برامج الحاسوب سواء كانت مثبتة على الحواسيب أو مخزنة في وسائط التخزين فإنها تعد من أصناف الأموال المتقومة التي لا يجوز التعدي عليها، وعدم حمايتها يعتبر هدرا لأحد الضروريات الشرعية وهي حفظ المال حيث قال عز وجل:﴿ وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ ﴾[1]، ولذلك يجرم التعدي على برامج الحاسوب بعقوبات تعزيرية متفاوتة بحسب جسامة الأضرار الملحقة ووفق ما يقدره الإمام وما يراه مناسبا.

وما يجب لفت النظر إليه أن بعض المسلمين يعتقدون أنه يحرم فقط الاعتداء على مال المسلمين بينما لا يحرم غصب مال الكفار وهذا اعتقاد خاطئ، فمن المعلوم شرعا أن أموال المعاهدين من ذميين وغير ذميين كأموال المسلمين لأن العهد يعصم الدم والمال والعرض، وبما أن الدول غير الإسلامية تنتمي لمنظمة الأمم المتحدة[2] فهي حكما دول معاهدة ورعاياها معاهدون ولا يجوز التعرض لشيء من أموالهم بالأخذ بغير حق شرعي، وبناء عليه تكون الشركات غير الإسلامية المنتجة للبرامج في حكم الشركات الإسلامية، فلا يجوز تقليد أو طبع أو نسخ مصنفات مملوكة للآخرين، ويكون هذا اعتداء يجب الحماية منه وإزالته احتراما لحقوق الآخرين وبعدا عن الإضرار بهم ما داموا غير حربيين[3].

وهو ما دعمته الفتوى الصادرة من اللجنة الدائمة للبحوث العلمية والإفتاء بالمملكة العربية السعودية[4]، بأنه لا يجوز نسخ البرامج التي يمنع أصحابها نسخها إلا بإذنهم ، لقوله ﷺ: (المسلمون على شروطهم)[5] ، ولقوله ﷺ: (لا يحل مال امرئ مسلم إلا بطيبة من نفسه)[6] ، وقوله ﷺ: (من

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

سبق إلى مباح فهو أحق به)[1] ، سواء كان صاحب هذا البرنامج مسلما أو كافرا غير حربي ، لأن حق الكافر غير الحربي محترم كحق المسلم[2].

وعلى ضوء ذلك فإنه لا يجوز شرعا التعدي على حماية برامج الحاسوب كما لا يجوز شرعا استنساخها بغرض المتاجرة بها أو الإضرار بأصحابها ويخضع المتعدي لعقوبات تعزيرية متفاوتة مع ضمان الضرر الذي ألحقه بأصحاب الحق.

المطلب الثالث: جريمة إنشاء ونشر الفيروسات الإلكترونية

تطرقت في الباب الثاني المتعلق بأنماط الجرائم الإلكترونية وآثارها إلى ماهية الفيروسات وأنواعها، كما تم التعرف النسبي على حجم الخسائر المادية والمعنوية التي يلحقها هذا النوع من البرامج الخبيثة بالمصالح العامة والخاصة، وتجنبا للتكرار فإنني سأكتفي بتعريف يضاف لما ذكر في موضوع الفيروسات وأنواع الأضرار التي تلحقها.

الفرع الأول: المقصود بفيروسات الحاسوب

يعرّف فيروس الحاسوب بأنه "عبارة عن برنامج يصممه المجرم المعلوماتي بطريقة تعطيه القدرة عل ربط نفسه ذاتيا ببرامج أخرى، ثم يتوالد ويتكاثر تلقائيا وينتشر داخل البرامج المختلفة أو بين مواقع معينة من ذاكرة الحاسب حتى يحقق الأهداف المتوخاة من نشره"[3].

فالفيروس عبارة عن برنامج يصممه المجرم المعلوماتي بطريقة تعطيه القدرة على ربط نفسه ذاتيا ببرامج أخرى أو بالنظام المعلوماتي حتى يحقق الأهداف التي أنشئ من أجلها، ويتميز الفيروس بعدة خصائص منها قدرة التخفي والتمويه على مستخدم النظام أو الحاسوب، وأيضا قدرته على الانتشار من حاسوب إلى آخر داخل شبكات الاتصال، بالإضافة إلى قدرته على التسلل إلى داخل النظم المعلوماتية واختراقها مباشرة أو عن طريق كسر نظم الحماية ومن ثم يقوم بإنجاز مهامه التخريبية؛

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كتدمير أو إتلاف أو محو أو طمس أو تغيير البيانات والمعلومات المخزنة على وسائط التخزين، أو التجسس وسرقة المعلومات، ولهذا يعد الفيروس شديد الصلة بالجريمة الإلكترونية بشكل عام كونه من أهم وسائل مجرمي المعلومات التي يعتمدون عليها في تحقيق جرائمهم.

الفرع الثاني: الحكم الشرعي للتعدي باستعمال الفيروسات

الفيروسات هي من النوازل التي برزت بظهور الحواسيب والأنظمة المعلوماتية والشبكات، ونظرا لما تؤول به من أضرار على الأموال والمصالح فإن الشريعة الإسلامية تعالج هذه الظاهرة باعتبار الضرر الذي تلحقه، وباعتبار التعدي على المال المتقوم وذلك كما يلي:[1]

1 ـــ يعد إتلاف البرامج والحواسيب وسرقة المعلومات من أبرز مقاصد نشر الفيروسات وهو تصرف محظور لدى جميع الهيئات والمنظمات والاتفاقات الدولية نظرا لما يلحقه من أضرار جسيمة بالضحايا. وإلحاق الضرر منهي عنه في الشريعة الإسلامية بنصوص صريحة وعلى رأسها قوله ﷺ: (لا ضرر ولا ضرار)[2] وهي قاعدة من قواعد الشريعة الإسلامية التي أصلها من شواهد الكتاب والسنة؛ حيث نهى الله سبحانه وتعالى عباده عن الظلم والعدوان في قوله عز وجل:﴿ وَلَا تَعْتَدُوٓاْ إِنَّ ٱللَّهَ لَا يُحِبُّ ٱلْمُعْتَدِينَ ﴾ [3]، وقد ورد في تفسير هذه الآية أنها تنهى عن العدوان في حالة الحرب مع الكفار من تقتيل للأطفال والنساء والشيوخ وإحراق الممتلكات[4]، هذا في حالة الحرب وهو ما ينص بالضرورة عدم إلحاق الضرر بالأموال والممتلكات والأنفس في سائر الأحوال، كما يعد الإضرار بالآخرين من باب الفساد في الأرض حيث نهى الله سبحانه وتعالى عن ذلك في قوله عز وجل:﴿ وَلَا تُفْسِدُواْ فِي ٱلْأَرْضِ بَعْدَ إِصْلَٰحِهَا ﴾ [5] ، وقوله تعالى:﴿ وَإِذَا تَوَلَّىٰ سَعَىٰ فِي ٱلْأَرْضِ لِيُفْسِدَ فِيهَا وَيُهْلِكَ ٱلْحَرْثَ وَٱلنَّسْلَ ۗ وَٱللَّهُ لَا يُحِبُّ ٱلْفَسَادَ ﴾ [6]، وما يشهد لقاعدة "لاضرر ولا ضرار" من السنة النبوية قوله ﷺ: (من ضار ضار الله به ومن شاق شاق الله عليه)[7] وهو حديث ينذر بالوعيد لكل من يتعمد في إلحاق الضرر بالغير.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ـــ كما تعالج الشريعة الإسلامية ظاهرة إنشاء ونشر الفيروسات باعتبار أن أجهزة الحاسوب من الأعيان المالية وبرامجه من المنافع مما يجعل كليهما يندرج ضمن الأموال المتقومة المعتدّ بها ـــ كما سبق شرحه ـــ والمعلوم عند جمهور الفقهاء أن المال كل ما كان منتفعا به وهو إما أعيان أو منافع[1]، ولأن حفظ المال من الضروريات الخمس التي تمنع الشريعة الإسلامية التعدي عليه سواء بالأخذ أو الإتلاف أو التخريب، فإن صورة التعدي عن طريق الفيروسات هو من باب أكل المال بالباطل والنص يحرم ذلك في قوله تعالى:﴿ وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ ﴾ [2]، كما قال عز وجل:﴿يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٍ مِّنكُمْ﴾[3]، وقد وردت أحاديث صريحة تفيد تحريم أكل أموال الناس بالباطل من بينها قوله ﷺ في حجة الوداع: (إن دماءكم وأموالكم حرام عليكم، كحرمة يومكم هذا، في شهركم هذا، في بلدكم هذا)[4]، وقال أيضا ﷺ : (كل المسلم على المسلم حرام، دمه وماله وعرضه)[5]، وبناء على ذلك أوجبت الشريعة الإسلامية في شأن أكل أموال الناس بالباطل أحكاما رادعة من تغريم وحدود وفرض الضمان على المتلف، ناهيك عن الوعيد بالجزاء الأخروي.

وبالنظر إلى ما تحدثه الفيروسات من مضار، فإن إنشاؤها ونشرها هو تعدٍ بغير حق على أموال الناس ـــ معصومي المال والدم ـــ وهو محرم ويستوجب العقاب التعزيري مع الضمان بالمثل أو القيمة على المتسبب، والضمان هو التزام بتعويض الغير عما لحقه من تلف المال أو ضياع المنافع، أو عن الضرر الجزئي أو الكلي الحادث بالنفس الإنسانية[6]، ومن المعلوم في الأصول أن ضمان المثليات بالمثل والقيميات بالقيمة وأن القواعد تقتضي أن يكون مقدار الضمان بقدر التالف[7]، فالمتعمد في إتلاف أموال الناس متوعد بالعقاب في الآخرة إضافة إلى العقوبة الدنيوية التي يفرضها الإمام وذلك بالسجن والتغريم إضافة إلى تعويض الضرر الذي يلحقه بالضحية[8].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني: جرائم التعدي على المواقع الإلكترونية

لقد أدى اتساع دائرة المعرفة والبحث في جميع مجالات الحياة إلى بروز العديد من المفاهيم والاستراتيجيات التي غيرت من أسس التفوق والنجاح، و أدت الزيادة الهائلة في كمية المعلومات المتوافرة إلى خلق ضرورة ملحة لوضع نظم متكاملة لهذه المعلومات كأساليب جديدة تكون قادرة على التعامل مع التقنية الحديثة لمعالجة البيانات وتخزين واسترجاع المعلومات.

وكان إنشاء وامتلاك المواقع الإلكترونية من أهم الأساليب الناجحة بالنظر إلى ما توفره من تيسير في تقديم الخدمات المختلفة للمجتمع المعلوماتي، وما تحققه من انخفاض في تكلفة الوقت والجهد فضلا عن انخفاض التكاليف المادية للمعاملات بالنسبة للمؤسسات الخاصة والحكومية والمجتمعات على حد سواء.

المطلب الأول: مفهوم الموقع الإلكتروني

الفرع الأول: المفهوم الاصطلاحي للموقع الإلكتروني

يعرّف الموقع web site بأنه عبارة عن مكان على الانترنت، يمكن أن تجد فيه معلومات عن شيء معين.[1] وعرّفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقع بأنه: مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد[2].

ومن خلال استقرائي للعديد من التعريفات الخاصة بالموقع الإلكتروني فإنه يمكن استنتاج أن الموقع الإلكتروني عبارة عن حيّز افتراضي ينشأ على شبكة الانترنت وتستضيفه إحدى الشركات المعتمدة أو مزودي الخدمة أو ما شابهها، وذلك بمقابل مالي لمدة معينة وقد يكون بدون مقابل، ويسمح الموقع لمستخدم الانترنت بمعاينة صفحاته المتعددة والاطلاع على محتوياته، كما يتيح إمكانية التعاقد الافتراضي أو التواصل وغيره. ويتخذ الموقع الإلكتروني صورا عديدة كأن يكون عبارة عن

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

مؤسسة تجارية كالمحلات الافتراضية، أو مؤسسة مالية كالبنوك، أو مؤسسة حكومية افتراضية، أومؤسسة طبية أو تربوية وغيرها وكلها تتمتع بالحصانة القانونية.

ويستوجب أن يحمل كل موقع على شبكة الانترنت علامة تميزه عن غيره من المواقع وهو ما يسمى بالنطاق أو اسم الدومين Le nom du domaine وهو يعادل تماما العلامة التجارية التي تميز السعلة أو الخدمة في مجال التجارة الإلكترونية[1].

وما يجب التنويه له أن من يقف وراء تسيير المواقع على شبكة الانترنت هم أشخاص مجهولون ذوو مسؤوليات محدودة قانونا من بينهم؛ متعهدي الوصول، ومتعهدي الإيواء، والمنتج، وناقل المعلومات، ومتعهد الخدمات، ومورد المعلومات وغيرهم، ويطلق على هؤلاء الأشخاص بـــ "مقدمو الخدمات الوسيطة"[2].

الفرع الثاني: صور التعدي على المواقع الإلكترونية

يتخذ التعدي على المواقع الإلكترونية أشكالا عديدة تتنوع بحسب أغراض الجاني من وراء تصرفه الإجرامي تجاه الضحية؛ كسرقة البيانات المخزنة أو البرامج أو الملفات الخاصة أو سرقة الأموال الإلكترونية، أو تعريض أمن دولة ما للخطر أو التلاعب بوسائل أمنها كاختراق نظم الملاحة الجوية أو البحرية ونحوها، أو تخريب مواقع الحكومات الإلكترونية ومواقع التجارة الإلكترونية. والتخريب معناه إتلاف الشيء محل الجريمة والتقليل من قيمته وجعله غير صالح للاستعمال أو تعطيله، أي تعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية، وهو إفناء لمادة الشيء فيصبح غير صالح إطلاقا للاستعمال في الغرض المخصص له، ومن ثم تضييع قيمته على المالك ومصلحة المستفيد، والعناصر التالية تبين أبرز صور التعدي على المواقع الإلكترونية:

1 ـــ الدخول غير المشروع للمواقع الإلكترونية والذي في الغالب يستخدم فيه برامج الاختراق وكسر مفاتيح الحماية بغرض إنجاز تصرفات معينة لها علاقة بالجرائم الإلكترونية كالتنصت والتجسس على الموقع الضحية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

2 ــ التعديل غير المشروع للمعلومات والبيانات وهي من أكثر صور الإتلاف شيوعا، ويقصد بها إجراء نوع من التغيير غير المشروع للمعلومات والبيانات المحفوظة على المواقع واستبدالها بمعطيات ومعلومات جديدة دون إذن المالك بهدف إحداث التشويش على صحة البيانات والمعلومات القائمة، أوتثبيت فيروس ما قد يكون الهدف من وراءه إتلاف المكونات المنطقية لأنظمة المتصفحين أو التجسس عليهم أو إتلاف الموقع بذاته.

3 ــ تدمير البيانات والمعلومات، وهي من أخطر صور التعدي على المواقع الإلكترونية وتشمل: محو جزء أو كل المعطيات المتعلقة بالموقع عن طريق اختراق قاعدة بياناته، نقل أو تخزين المعلومات محل الحماية إلى دعامات خاصة بالجاني، الإتلاف الكلي أو الجزئي لمعلومات الموقع، تعطيل الموقع عن أداء وظيفته لفترة معينة أو بصفة نهائية.

4 ــ تدمير المواقع الإلكترونية، وذلك عن طريق ضخ مئات الآلاف من الرسائل الإلكترونية (e-mails) من حاسوب الجاني إلى الموقع المستهدف بغرض التأثير على السعة التخزينية للموقع، حيث تشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطاً يؤدي في النهاية إلى تفجير موقع الضحية فتتشتت البيانات والمعلومات المخزنة فيه مما يتيح نقلها إلى جهاز المعتدي، كما تمّكن هذه العملية الجاني من حرية التجول في الموقع المستهدف والحصول على ما يحتاجه من أرقام ومعلومات وبيانات خاصة.[1]

المطلب الثاني: حكم التعدي على المواقع الإلكترونية

الفرع الأول: أنواع المواقع الإلكترونية

يخضع تقسيم أنواع المواقع الإلكترونية لاعتبارات متعددة؛ كتقسيمها بحسب الموضوعات إلى إخبارية وتعليمية، وحكومية ونحوها، كما يمكن تقسيمها باعتبار الاستعمال إلى مواقع مجانية ومواقع غير مجانية، أو تقسيمها حسب الامتداد الذي تنتمي إليه كالمواقع التجارية، والمواقع الحكومية،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والمواقع التعليمية ونحوها، إلا أن التقسيم الذي يخدمنا في هذا المطلب، هو تقسيم المواقع باعتبار المصالح والمفاسد إلى مواقع نافعة للناس، ومواقع تضر بهم.

أولا: المواقع الإلكترونية النافعة

المقصود بالمواقع النافعة ذات العلاقة بالبحث، كل المواقع الملتزمة بالضوابط الشرعية أو التي لا تخرج عن دائرة الشرع ومن شأنها أن تخدم البشرية وتلبي حاجاتها في جميع الميادين سواء الدينية، أو الاجتماعية، أو الاقتصادية، أو الثقافية، أو العلمية وغيرها مما يجلب التيسير للناس، لأن التيسير هو من أعلى مقاصد التشريع الإسلامي؛ فما من حكم من الأحكام الشرعية العملية إلا وتضمن جانب التيسير، ومن أدلة ذلك قوله سبحانه وتعالى بعد تشريع الصيام:﴿ يُرِيدُ ٱللَّهُ بِكُمُ ٱلْيُسْرَ وَلَا يُرِيدُ بِكُمُ ٱلْعُسْرَ وَلِتُكْمِلُواْ ٱلْعِدَّةَ وَلِتُكَبِّرُواْ ٱللَّهَ عَلَىٰ مَا هَدَىٰكُمْ ﴾ [1]؛ وبعد تشريع أحكام الطهارة قال عز وجل:﴿مَايُرِيدُ ٱللَّهُ لِيَجْعَلَ عَلَيْكُم مِّنْ حَرَجٍ وَلَٰكِن يُرِيدُ لِيُطَهِّرَكُمْ وَلِيُتِمَّ نِعْمَتَهُۥ عَلَيْكُمْ لَعَلَّكُمْ تَشْكُرُونَ﴾[2]، وبعد الأمر بالجهاد قال عز وجل:﴿ هُوَ ٱجْتَبَىٰكُمْ وَمَا جَعَلَ عَلَيْكُمْ فِى ٱلدِّينِ مِنْ حَرَجٍ﴾[3]، ومن السنة النبوية الشريفة أن عائشة رضي الله عنها قالت: "ما خُيّر رسول الله ﷺ بين أمرين قط إلا أخذ أيسرهما ما لم يكن إثماً؛ فإن كان إثماً كان أبعد الناس منه، وما انتقم رسول الله ﷺ لنفسه في شيء قط إلا أن تُنتَهك حرمة الله فينتقم بها لله"[4].

وبناء على ذلك فإن المواقع الإلكترونية النافعة في الشريعة الإسلامية تقوم على عنصرين أساسيين؛ أولهما أن يكون الموقع يؤدي منفعة مباحة شرعا إذ أن من شرط المال في الشريعة الإسلامية أن يكون ذا منفعة مباحة، ومن شرط الضمان في مسائل الإتلاف أن يكون المال متقوّماً أي يكون ذا قيمة معتبرة شرعا[5]، والعنصر الثاني أن يكون صاحب الموقع معصوم المال والدم، وهو المسلم والذمي والمعاهد والمستأمن، فلا يجوز التعدي على أموال هؤلاء؛ لأن الله سبحانه وتعالى قد حفظ أموالهم وحرّم الاعتداء عليها.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثانيا: المواقع الإلكترونية الضارة

وهي المواقع التي اختل فيها أحد أو كلا العنصرين السابقين، فإما أن تكون مواقع تحتوي على منفعة محرمة كالمواقع التي تتاجر بالمحرمات ونحوها، أو مواقع يملكها الحربيون أو تخدم مصالحهم ضد المسلمين كالمواقع المغرضة والمواقع الإرهابية والمواقع التي تنتهك حرمات الأديان السماوية.

الفرع الثاني: حكم الشريعة في التعدي على المواقع الإلكترونية

أولا ــ حكم التعدي على المواقع النافعة:

لقد نهى الله سبحانه وتعالى عن الاعتداء على الآخرين في قوله عز وجل:﴿ وَلَا تَعْتَدُوٓاْ إِنَّ ٱللَّهَ لَا يُحِبُّ ٱلْمُعْتَدِينَ ﴾ [1]، وهو دليل صريح على حفظ الحقوق وصيانتها، وما دامت المواقع الإلكترونية النافعة حق للآخرين فلا يجوز الاعتداء عليها بأي وجه من الاعتداء، ولذلك فإن إتلاف هذه المواقع يعد من أنواع الاعتداء المحرم، وهو حكم يدعمه قرار مجمع الفقه الإسلامي الذي صدر في دورته الخامسة سنة 1409هـ بأن حقوق التأليف والاختراع أو الابتكار مصونة شرعاً ولأصحابها حق التصرف فيها ولا يجوز الاعتداء عليها[2]. وهو حكم يفيد أن الاعتداء على المواقع الالكترونية النافعة ممنوع شرعاً من باب أولى ، فإذا كان حق الاختراع والابتكار مصوناً شرعاً ، فكذلك الموقع على شبكة الانترنت مصون شرعاً ولا يجوز الاعتداء عليه.

وبناء على ذلك إذا تم اختراق الموقع الالكتروني النافع أوتدميره بشتى الصور المذكورة سلفا فإن الجاني يعاقب وذلك بإلزامه بضمان ما أتلفه من برامج ومعلومات وبيانات، والضمان يكون بدفع قيمة كل ما كان قيمياً، وبالمثل ما كان مثلياً ــ كأن يعيد الموقع إلى حالته الأصلية إن حفظ منه نسخة قبل الإتلاف ــ، بالإضافة إلى خضوع الجاني إلى عقوبة التعزير لأن التعدي من الأمور المحرمة بالكتاب والسنة والإجماع وعلى ذلك فإن للقاضي الحرية في أن يعزر الجاني بما يراه مناسباً من العقاب تأديبا له وردعاً لغيره من الإقدام على مثل هذه الأفعال[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثانيا: حكم التعدي على المواقع الضارة.

من الناحية الشرعية لا خلاف في أن هذه المواقع لا مالية لها إذا ثبت أنها تنافي أحكام الشريعة الإسلامية ومقاصدها، كما أنه لا خلاف في عدم وجوب الضمان فيها، إلا أن هناك تحفظا من بعض الفقهاء المعاصرين حول مدى مشروعية تخريب وتدمير هذه المواقع، حيث استندوا في ذلك إلى قياس المصالح والمفاسد، وقد تم الرد على ذلك في أن مشروعية تدمير هذه المواقع يكون وفق ضوابط معينة وبيان ذلك كما يلي:

جواز تدمير المواقع الإلكترونية التي تسبب الضرر بالدين أو الأخلاق أو أحد مقاصد الشريعة الإسلامية ولا يرى العلماء الضمان على من أتلفها، حيث يقول ابن القيم[1] رحمه الله: "وكذلك لا ضمان في تحريق الكتب المضلة وإتلافها ... وقد رأى النبي ﷺ بيد عمر بن الخطاب رضي الله عنه كتاباً اكتتبه من التوراة وأعجبه موافقته للقرآن، فتمعرّ وجه النبي ﷺ حتى ذهب به عمر رضي الله عنه إلى التنور فألقاه فيه[2]، فكيف لو رأى النبي ﷺ ما صنف بعده من الكتب التي يعارض بها ما في القرآن والسنة ؟ والله المستعان. وكل هذه الكتب المتضمنة لمخالفة السنة غير مأذون فيها، بل مأذون في محقها وإتلافها، وما على الأمة أضر منها، وقد حرّق الصحابة جميع المصاحف المخالفة لمصحف عثمان رضي الله عنه لما خافوا على الأمة من الاختلاف، فكيف لو رأوا هذه الكتب التي أوقعت الخلاف والتفرق بين الأمة... إلى أن قال : والمقصود أن هذه الكتب المشتملة على الكذب والبدعة يجب إتلافها وإعدامها، وهي أولى بذلك من إتلاف آلات اللهو والمعازف، وإتلاف آنية الخمر، فإن ضررها أعظم من ضرر هذه، ولا ضمان فيها كما لا ضمان في كسر أواني الخمر وشق زقاقها"[3].

وقياس على ذلك فإنه لا ضمان في تدمير الضار من المواقع الإلكترونية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أما التحفظ المتعلق بترجيح المصالح أو المفاسد باعتبار أن تدمير هذه المواقع قد يؤدي بأصحابها إلى الانتقام فيدمرون مواقع أهل الإسلام والمواقع النافعة، ففي هذه الحالة يجب أن يقدّر الأمر بقدره لأنه من شروط إزالة المنكر ألا يترتب على إزالته منكر أكبر، فإن كان يترتب على إزالة المنكر منكر أكبر منه فلا يزال، كما أن مسؤولية أهل العلم والاختصاص تنحصر في رفع التقارير إلى المصالح العامة ـــ مصالح الدولة ـــ باعتبارها المسؤول الوحيد المخول له اتخاذ الإجراءات اللازمة تجاه المواقع الضارة وهذا تجنبا لانفلات الرأي والتصرف العشوائي الذي عادة ما يعود بالسلب على الإسلام والمسلمين، والعلاج الأفضل لذلك يكون باتخاذ وسائل الحذر والحماية العامة عن طريق حجب المواقع الضارة في الدول الإسلامية، بالإضافة إلى تطوير برامج الحماية ونشر الوعي والحذر العام. وخير مثال على ذلك ما سعت إليه المملكة العربية السعودية ممثلة في مدينة الملك عبد العزيز للعلوم والتقنية حيث عملت على حجب المواقع الضارة كالمواقع الإباحية وهو أقل عمل يمكن فعله لمواجهة ضرر المواقع الإباحية والمضللة، وعلى الدول الإسلامية الأخرى أن تحمي شعوبها من خطر هذه المواقع بالسعي لحجب المواقع الضارة بالدين والأخلاق رعاية للأمة وقياماً بالواجب، لأن من حقوق الرعية على الراعي سد أبواب الفساد عن البلاد والعباد[1].

ولقد صدر في هذا الشأن فتوى من طرف هيئة العلماء[2] بالمملكة العربية السعودية حول حكم تعطيل المواقع التي تعادي الإسلام والأخلاق وتخريبها جاء فيها: " شبكة الانترنت هذه من وسائل الاتصالات الحديثة السريعة في إيصال المعلومات الواسعة من حيث الانتشار وسهولة الوصول إليها، وهي إن استغلت في الخير والدعوة إلى الله ونشر دين الله في أصقاع الأرض من قبل الأفراد والمؤسسات الإسلامية المختلفة ، فلا شك أنها من الجهاد في سبيل الله بالبيان واللسان ويجب على المسلمين استغلالها وتسخيرها لهذا الغرض الخير، أما المواقع الفاسدة المخلة والمضرة بعقائد المسلمين من خلال التلبيس والتشكيك، والمضرة بأخلاقهم كذلك من خلال ما يعرض فيها من الدعوة إلى الفساد وتيسير طرقه وتعليم الناشئة لهذه الأمور، وتربيتهم عليها من خلال ما يعرض فيها... فلا ريب أن هذا من أعظم المنكرات التي يجب التصدي لها وإنكارها وفق قواعد إنكار المنكر التي جاء بها النص

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

من الكتاب والسنة، وبيّنها وفصلها علماء الأمة والله تعالى يقول:﴿ وَلْتَكُن مِّنكُمْ أُمَّةٌ يَدْعُونَ إِلَى ٱلْخَيْرِ وَيَأْمُرُونَ بِٱلْمَعْرُوفِ وَيَنْهَوْنَ عَنِ ٱلْمُنكَرِ ۚ ﴾ [1]. وقال ﷺ كما في الحديث الذي رواه أبو سعيد الخدري[2] رضي الله عنه : (من رأى منكم منكراً فليغيره بيده، فإن لم يستطع فبلسانه فإن لم يستطع فبقلبه، وذلك أضعف الإيمان)[3].

فمن اطلع على موقع من هذه المواقع فوجد فيها تلك المفاسد فليغيرها حسب ما يقتضيه الحال، لأن هذا ضرر، والضرر إن كان يزول من غير ضرر وجب إزالته، وكذا إن زال بضرر أخف منه، أما إن لم يزل إلا بضرر أعلى وأكثر فلا يزال بل يتحمل أدنى الضررين لدفع أعلاهما... فإن كانت محاربة مواقع الفساد بمثل هذه الفيروسات لا ينتج عنها ضررا أكبر من ضرر وجود تلك المواقع، فإن هذا من أعمال القربات ، ومن الجهاد في سبيل الله"[4].

والخلاصة أنه لا يجوز التعدي على المواقع الإلكترونية النافعة لما تكتسبه من حرمة شرعية فاختراقها هو بمثابة اقتحام بيت دون إذن من أهله ناهيك إن صاحب ذلك الاقتحام الإتلاف والتدمير، كما يجوز تدمير المواقع الإلكترونية التي تسبب الضرر بالدين أو الأخلاق أو أحد مقاصد الشريعة الإسلامية على أن لا يترتب على إزالة المنكر منكرا أكبر منه وهو عمل مخول لمؤسسة الدولة، وما يجب التنويه له أن تحديد الحربي من غيره ليس لآحاد الناس بل هو راجع إلى الهيئات النظامية من القضاء والمصالح الأمنية في هذه الأزمنة التي أصبحت فيها أغلب الدول دولاً معاهدة لا حربية، وعلى ذلك لا يجوز الإقدام على التدمير والاختراق بمجرد أخبار تتداول بين عامة الناس، أو نداءات تطلق في هذا المنتدى أو ذاك من غير رجوع إلى أهل الحل والعقد، وذلك استئناسا بقوله تعالى:﴿ وَإِذَا جَآءَهُمْ أَمْرٌ مِّنَ ٱلْأَمْنِ أَوِ ٱلْخَوْفِ أَذَاعُواْ بِهِۦ ۖ وَلَوْ رَدُّوهُ إِلَى ٱلرَّسُولِ وَإِلَىٰٓ أُوْلِى ٱلْأَمْرِ مِنْهُمْ لَعَلِمَهُ ٱلَّذِينَ يَسْتَنۢبِطُونَهُۥ مِنْهُمْ ۗ وَلَوْلَا فَضْلُ ٱللَّهِ عَلَيْكُمْ وَرَحْمَتُهُۥ لَٱتَّبَعْتُمُ ٱلشَّيْطَٰنَ إِلَّا قَلِيلًا ﴾ [5]. [6]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث: جرائم التزوير الإلكتروني

لقد تنوعت أساليب الجرائم الإلكترونية وتعددت اتجاهاتها حتى أصبحت من أخطر ما يهدد المصالح والحقوق لاسيما تلك التي تقوم على أساس تثبيت المعلومات والبيانات والتي كثيرا ما تكون عرضة للاعتداءات عن طريق تزوير مضمونها والذي من شأنه إحداث أضرار مادية أو معنوية بالمصالح العامة والخاصة، ولذلك يعد التزوير الإلكتروني من أخطر طرق الغش التي تقع في مجال المعالجة الآلية للبيانات وذلك كنتيجة لما تتيحه التكنولوجيا من إمكانات في هذا المجال.

المطلب الأول: مفهوم التزوير الإلكتروني

الفرع الأول: تعريف التزوير في اللغة

التزوير لغة "هو فعل الكذب والباطل، ومنه تشبيه غير الأصل بأصله بالتهيئة والتحسين للإيهام، وهو مشتق من تزوير الصدر، والمزَّور من الإبل الذي سله من بطن أمه، أعوج الصدر فيغمزه ليقيمه فيبقى فيه من غمزه أثر يعلم أنه مزوَّر، وتزاور عنه عدل عنه وانحرف " قال تعالى:﴿ تَّزَوَرُ عَن كَهۡفِهِمۡ﴾[1]، وقيل هو التمويه من موّه الحديد أي طلاه بالذهب ليظهر أنه ذهب، فهو تمويه الأصل والانحراف عن الدليل[2].

الفرع الثاني: التزوير في الاصطلاح الفقهي

يعرّف التزوير اصطلاحا بأنه: "تحسين الشيء ووصفه بخلاف صفته حتى يخيل إلى من سمعه أو رآه أنه بخلاف ما هو به، فهو ميل عن الحق وتمويه الباطل بما يوهم أنه حق" وهو تعريف اعتمده الكثير من علماء الشريعة الإسلامية لشموليته حيث يضم التزوير بشقيه القولي والفعلي[3]، فالقولي كشهادة الزور (أي القول الكاذب) والفعلي كالتزوير بتغيير ما ثُبت بالكتابة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثالث: تعريف التزوير في القانون الوضعي

عرّف التزوير في القانون الوضعي بأنه "تغيير الحقيقة بقصد الغش، وبإحدى الطرق التي عينها القانون، تغييرا من شأنه أن يسبب ضررا"[1]، وهو تعريف يشمل معظم تعريفات القوانين الوضعية العامة.

وما يمكن استخلاصه من خلال هذه التعريفات أن التزوير هو فعل غير مأذون به يقوم على تحريف الحقائق بالكتابة أو شهادة الزور ليوهم المتلقي بأنه حق وذلك عن طريق الغش وتغيير الحقيقة ليثبت خلافها من أجل تحقيق مصلحة ما، مما يترتب عليه الظلم والإضرار بالغير.

الفرع الرابع: تعريف التزوير الإلكتروني

يعرّف التزوير الإلكتروني بأنه "تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية استعمالها"[2].

ويفهم من ذلك أن التزوير الإلكتروني هو أي تغير للحقيقة يرد على مخرجات الحاسب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة، أو كانت مرسومة عن طريق الماسح الضوئي، كما يستوي في المحرر الإلكتروني أن يكون مدونا باللغة العربية أو أي لغة أخرى لها دلالتها، وشرط أن يكون المحرر الإلكتروني ذا أثر في إثبات حق أو أثر قانوني معين[3].

كما يعرّف التزوير الإلكتروني من ناحية الإجراءات، "بأنه تغيير البيانات والمعلومات في المستندات المعالجة آليا باستخدام أجهزة وبرمجيات اختراق تُعد للحصول على مستندات تحاكي الأصل ولكن مزورة في مضمونها وصيغتها بنية استخدامها في تحقيق مصلحة لمرتكب التزوير أو لشخص آخر"[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وهو تعريف يفيد وقوع التزوير الإلكتروني على المحررات الإلكترونية التي هي بمثابة أداة لإثبات حق من الحقوق وهذا ما سيبينه المطلب التالي.

المطلب الثاني: طبيعة المحررات الإلكترونية

إن جرائم التزوير المعلوماتي هي من أخطر صور الغش التي أثارت الشك حول دلالة المحررات الإلكترونية في الإثبات[1]، فبفضل تقدم الأدوات المساعدة للحاسوب أصبح من السهل نقل الصور الشخصية والتوقيعات والنصوص وإعادة معالجتها كيفما يريده المزور، وقد شهد التطبيق العلمي لنشاط الحاسوب حالات تزوير مضمونها إبرام صفقات وهمية بأسماء أشخاص آخرين[2]، أو طلب وشراء سلع أو خدمات بأسماء أشخاص مزورة وغيرها[3]، كما أصبح من السهل جدا على كل محترف وهاوي أن يقوم بمعظم أشكال التزوير المادية والمعنوية التي كانت مستعصية سابقا كالتقليد، والتوقيع، والحذف، والإضافة، والتعديل أوالتغيير..

ولتتحقق جريمة التزوير المعلوماتي فإنه يشترط أن تكون المحررات الإلكترونية ذات قيمة إثباتية سواء كانت المحررات عبارة عن سجلات رقمية أو وثائق تم معالجتها إلكترونياً وهو إجراء يدخل ضمن نطاق الحماية الجنائية للنظام المعلوماتي حيث يتفق مع القواعد العامة للجريمة التقليدية لإثبات الحقوق، إذ يشترط في المحرر المزور أن يكون أداة لإثبات حق من الحقوق[4]، وهو ينطبق على المحررات الإلكترونية التي سأبين أهم أنواعها في الفروع التالية:

الفرع الأول ــ العقود الإلكترونية:

من المتعارف عليه أن العقد في الفقه الإسلامي يطلق على توافق إرادتين: إرادة الموجب، وإرادة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

القابل على وجه مشروع يثبت أثره في المحل المعقود عليه: كالبيع والإجارة[1]، بمعنى أن العقد يعبر عن تلاقي إرادتين على إحداث أثر مشروع يصبح إلزاميا بعد توافق الإيجاب والقبول، ورغم تعدد التعريفات المتعلقة بالعقد الإلكتروني إلا أن جميعها يتفق على أن هذا النوع من العقود يحصل بين طرفين عبر مجلس عقد افتراضي ويتم فيه الإيجاب والقبول عبر الوسائل الإلكترونية، ومن بين هذه التعريفات أن العقد الإلكتروني هو: "تنفيذ أو إبرام كل المعاملات التجارية في السلع والخدمات التي تتم بين مشروع تجاري وآخر أو بين تاجر ومستهلك، وذلك باستخدام تكنولوجيا المعلومات والاتصالات"[2]، كما عرّفه البعض بأنه "اتفاق يبرم وينفذ جزئيا وكليا عبر شبكة اتصالات دولية باستخدام التبادل الإلكتروني للبيانات، بقصد إنشاء التزامات تعاقدية، وذلك بإيجاب وقبول يمكن التعبير عنهما من خلال ذات الوسيط"[3]، كما يعرّف أيضا بأنه "عقد يتحقق بإيجاب وقبول مثل العقود العادية التي تبرم وتوقع كتابة، غير أن الإيجاب والقبول يتحقق بوسيلة إلكترونية دون حاجة إلى مستند مكتوب"[4]، وفي كل الأحوال فإن الكتابة الإلكترونية والتوقيع الإلكتروني لهما تأثير كبير على شكليات العقد الإلكتروني، حيث أن جميع المحررات والمستندات الورقية التي يتبادلها الأطراف عند إبرام العقد الإلكتروني يمكن تحويلها إلى محررات إلكترونية بعد توثيقها بتوقيع إلكتروني محمي من طرف جهات قانونية مختصة باعتماد شهادات التوثيق[5].

ولذلك فإن العقد الإلكتروني يتميز عن العقد التقليدي؛ بأنه عقد يتم بين حاضرين من حيث الزمان وغائبين من حيث المكان، كما يتميز العقد الإلكتروني بالطابع الدولي لأنه غالبا يتم عبر الشبكة العالمية ـــ الانترنت ـــ، كما يمكن تثبيت العقد الإلكتروني عن طريق الكتابة داخل المحرر الإلكتروني وتوقيع أطرافه إلكترونيا باعتبار أن المحرر الإلكتروني هو المرجع بالنسبة لما اتفق عليه الطرفان وتحديد التزاماتهما حيث يضفي التوقيع صفة الجدية على هذا المستند، كما يتصف العقد الإلكتروني غالبا بطابع التجارة لذا يطلق عليه عقد التجارة الإلكترونية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ونظرا للتوسع في التعامل التجاري الإلكتروني حول العالم، فإن الاتفاقات الدولية والتشريعات الحديثة بشأن تنظيم التجارة الإلكترونية تشترط توفر السجل الإلكتروني[1] عند القيام بالمعاملات الإلكترونية وهذا من أجل حفظ المعلومات المتبادلة بين أطراف التعامل وتوثيق البيانات المدونة فيه، كما حرصت معظم الاتفاقات النموذجية للتبادل الإلكتروني للبيانات على إلزامية الاحتفاظ بسجل إلكتروني يمكن الرجوع إليه عند الحاجة لاستعماله كأداة لإثبات حق من الحقوق، حيث أكدت على وجوب التخزين بدون تعديل أو تحريف، مع استخدام وسائل الأمان، على أن يكون السجل الإلكتروني كاملا ومتسلسلا زمنيا لجميع رسائل البيانات التي يتبادلها الأطراف إلكترونيا أثناء القيام بالعملية التجارية[2].

الفرع الثاني ــ المحررات الخدمية:

تقدم شبكة الانترنت الكثير من الخدمات الإخبارية والبحثية التي تنتقل عبر محررات إلكترونية تحمل ما يعبر عنه من أفكار ومعان، ومن أهم الخدمات التي تعتمد على المحررات الإلكترونية:

1 ــ شبكة الويب العالمية World Wide Web، وهي إحدى خدمات الانترنت التي تسمح بنقل الوثائق واستعمالها عن طريق وسيط إلكتروني يعتمد لغة عالمية تعرف بـــ (HTML) التي من خلالها يسهل الإبحار في مختلف المواقع الموجودة على شبكة الانترنت، وتحتوي شبكة الويب العالمية على كم هائل من المحررات والمستندات الإلكترونية المحفوظة التي تسمح لأي شخص وأية جهة الإطلاع عليها إذا كانت متاحة للجميع[3].

2 ــ البريد الإلكتروني Electronical Mail (e-mail) ، وهو من الخدمات الأكثر شيوعا واستعمالا على شبكة الانترنت، حيث بإمكان أي شخص من العالم إنشاء بريد إلكتروني يستقبل فيه رسائله الخاصة، ويتميز البريد الإلكتروني بسرعة تلقي المراسلات من أي مكان من العالم حيث تصل

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

في غضون بضع ثوان، الأمر الذي جعله من أهم الوسائل لإبرام العقود الإلكترونية[1].

3 ــ المواقع الإخبارية News Site ، هي مواقع خدمية تقوم بتوزيع نشرات إخبارية موجزة على مستخدميها عن طريق البريد الإلكتروني، حيث يمكن من خلالها التعرف على آخر المستجدات في جميع المجالات الاقتصادية والعلمية والسياسية وغيرها.

4 ــ مواقع المحادثات الفورية Chat ، هي عبارة عن مواقع خدمية تتيح إمكانية تبادل الآراء والمناقشات بطرق فورية حول أي موضوع كان حيث يتواصل المشاركون فيها بواسطة الكتابة مستعملين في ذلك أجهزة الحواسيب المتصلة بشبكة الانترنت[2] وقد تم تطويرها لتمكين الحوار عن طريق الاتصال السمعي البصري بين المشاركين.

الفرع الثالث: المحررات المالية

استطاع القطاع المالي والمصرفي الاستفادة من تقنية المعلومات والاتصال لما تتيحه من تيسير الخدمات المالية على المستوى المحلي والدولي، وهو ما كان له انعكاس مباشر على أعمال البنوك حيث انتشرت العديد من الخدمات المالية الإلكترونية التي استحسنها الناس بالنظر إلى ما تقدمه من تيسير في الحياة المعاصرة، ومن صور الخدمات المالية الإلكترونية ما يلي:

1 ــ البنوك الإلكترونية: يشهد العالم تطورا كبيرا في مجال الصناعة المصرفية وأدواتها حيث تحولت معظم الأجهزة المصرفية في العالم إلى نظم الصيرفة الإلكترونية في التعامل مع الأطراف المختلفة من أجل رفع مستوى الخدمة المصرفية والحصول على درجة عالية من رضا المتعاملين، وتشير دراسات بحثية أن نحو 65 بالمائة من إجمالي البنوك على مستوى العالم تمتلك مواقع خدمية على شبكة الانترنت[3]، وقد نتج عن ذلك تزايد عدد العمليات البنكية الإلكترونية وظهور ما يعرف بالبنوك الإلكترونية E-Banking التي توفر كافة الخدمات المصرفية من سحب وإيداع وتحويل وذلك من خلال قنوات التوزيع المعتمدة على شبكة الانترنت، وهو ما يجعلنا تصور مدى حجم المحررات الإلكترونيـــة

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ودرجة حساسيتها الأمنية.

2 ــ الاعتمادات المالية الإلكترونية؛ هي طريقة تستخدم في عمليات التجارة الإلكترونية حيث يقوم المستورد بإرسال طلب فتح الاعتماد إلكترونيا لدى بنكه ويقوم البنك بالرد عليه إلكترونيا (مع مراعاة الضوابط الشرعية في المعاملات المالية عند المسلمين)، وفي حالة الاتفاق يتم إرسال نص الاعتماد إلكترونيا إلى المستفيد، ويتم إرسال الفواتير الخاصة بعملية الشحن إلكترونيا، كما يقوم المستفيد بمراسلة الأطراف المشاركة في عملية البيع وتبليغهم بإرسال مستنداتهم إلكترونيا إلى البنك مصدر الاعتماد والذي بدوره يضمن لهم تحصيل قيمة الخدمات والسلعة محل التعاقد إذا استوفت الشروط المحررة على العقد الإلكتروني[1].

3 ــ التحويلات المالية الإلكترونية؛ هي عمليات إلكترونية تتم عن طريق توجيه أمر من المدين إلى البنك بالوفاء من حسابه إلى دائنه باتخاذ الإجراءات المصرفية اللازمة لتحويل مبلغ معين لحساب بنك المستفيد، أو توجيه الدائن أمرا إلكترونيا إلى بنكه بتحصيل مبلغ من حساب مدينه بناء على تفويض مسبق بواسطة محرر إلكتروني، وهي أوامر تعتبر من قبيل المحررات أو المستندات الإلكترونية التي من شأنها أن تحمل أثرا قانونيا بين أطراف التعامل.

4 ــ محررات الدفع والوفاء الإلكترونية؛ وهي من وسائل الدفع الجديدة التي عرفها القطاع المصرفي الحديث كانعكاس للتطور التكنولوجي، منها بطاقات الائتمان التي تمكّن حاملها من الدفع والوفاء إلكترونيا بضمان البنك المصدّر لها (مع التقيد بالضوابط الشرعية عند المسلمين)، وهي بطاقات بلاستيكية مجهزة بشرائح إلكترونية يخزن فيها مجموعة من البيانات التي تتضمن معلومات عن العميل حامل البطاقة والبنك المصدر لها وحدود المبلغ المسموح به للتعامل بها وتاريخ انتهاء صلاحيتها وغيرها من البيانات التي تنظم عملية التعامل بها، ولقد أجمع معظم المختصين في أنظمة الدفع الإلكتروني باعتبارها من المحررات الإلكترونية[2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وما نستخلصه بعد استقرائنا لكل هذه الأمثلة فإن كل المحررات الإلكترونية هي عبارة عن حقوق وأملاك تامة لأصحابها لا يجوز التعدي عليها بأي طريقة كانت كما لا يجوز نقلها للغير إلا بالطرق المشروعة.

المطلب الثالث: حكم التزوير وأدلته

إن شهادة الزور والتزوير مؤداهما معنى واحد لدى المذاهب الأربعة[1]، ولقد سمى الأصوليون شهادة الزور بالتزوير وأن من يعود عن شهادة الزور فلابد أن يعترف بتزويره ويعود عنه[2]، والتزوير منهي عنه ما دام الغرض منه إثبات الباطل وإبطال الحق.

والأصل في التزوير أنه محرم شرعا بكل صوره وأشكاله، سواء أكان ذلك بالقول كشهادة الزور أم بالفعل كتزوير الوثائق والمستندات ونحوها، ولقد صنفته الشريعة الإسلامية ضمن أكبر الكبائر وأشد المحرمات وهذا باتفاق فقهاء المذاهب الأربعة لاقتران التزوير وشهادة الزور بالإشراك بالله وعبادة الأوثان حيث قال عز وجل:﴿ إِنَّ ٱللَّهَ لَا يَغۡفِرُ أَن يُشۡرَكَ بِهِۦ وَيَغۡفِرُ مَا دُونَ ذَٰلِكَ لِمَن يَشَآءُۚ وَمَن يُشۡرِكۡ بِٱللَّهِ فَقَدِ ٱفۡتَرَىٰٓ إِثۡمًا عَظِيمًا ﴾[3]، وقد ثبت تحريم التزوير من القرآن الكريم، والسنة النبوية الشريفة ومن المعقول كما يلي:

الفرع الأول: تحريم التزوير في القرآن الكريم

تعرض القرآن الكريم لتحريم التزوير في آيات كثيرة منها:

قوله تعالى:﴿ فَٱجۡتَنِبُواْ ٱلرِّجۡسَ مِنَ ٱلۡأَوۡثَٰنِ وَٱجۡتَنِبُواْ قَوۡلَ ٱلزُّورِ ﴾ [4]، وهي من أكثر الآيات التي اعتمد عليها الفقهاء في تحريم التزوير باعتباره من الكبائر، حيث قرن الله عز وجل بين التزوير وعبادة الأوثان التي تعد من الكبائر فانسحب حكمها على التزوير؛ فالمشرك يزعم أن الأوثان تحقق له ما يريد

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

من خلال تحسينه للباطل الذي يجعل الناس يظنون أنه حقا، وكذلك التزوير حسّن الباطل حتى يظهر أنه حق لدى الغير فيصل الظالم لمبتغاه[1].

وقال تعالى:﴿ فَقَدْ جَآءُو ظُلْمًا وَزُورًا ﴾[2]، حيث جاء في تفسير الآية أن اليهود كذبوا وقيل نفر من الكفار، بافترائهم على الله بالباطل مع علمهم أنه باطل وقالوا عن الحق أنه افتراء، وقاموا بقلبه فجعلوا الباطل حقا ونسبوه بعد ذلك إلى رسول الله ﷺ[3].

وقال عز وجل:﴿ وَٱلَّذِينَ لَا يَشْهَدُونَ ٱلزُّورَ وَإِذَا مَرُّواْ بِٱللَّغْوِ مَرُّواْ كِرَامًا ﴾[4]، وهي آية تتحدث عن بعض صفات الصالحين، ومن صفاتهم أنهم لا يشهدون الباطل، وقيل: الإشراك وعبادة الأصنام وقيل الكذب والفسق والكفر الذي هو الزور، و لم يتمسكوا إلى بطريق الصدق[5].

وقوله تعالى:﴿ وَإِنَّهُمْ لَيَقُولُونَ مُنكَرًا مِّنَ ٱلْقَوْلِ وَزُورًا ۚ وَإِنَّ ٱللَّهَ لَعَفُوٌّ غَفُورٌ ﴾[6]، وهي آية جاءت في سياق الحديث عن الظهار وما يتعلق به، ووجه الاستدلال من الآية: أن المُظاهر استعمل الزور بقلبه للحق باطلا حيث جعل من الحقيقة الزوجية باطلا بجعل زوجته كأمه وما يترتب على ذلك من أحكام تحريمها عليه، وهذا أساس قلبه للحق[7].

الفرع الثاني: أدلة تحريم التزوير من السنة الشريفة

قال رسول الله ﷺ : (ألا أنبئكم بأكبر الكبائر؟ قلنا: بلى يا رسول الله، قال: الإشراك بالله وعقوق الوالدين، وكان متكئا فجلس، فقال: ألا وقول الزور وشهادة الزور، فما زال يكررها حتى قلنا ليته سكت)[8]، فقد بين النبي ﷺ أن الزور من أكبر الكبائر لما فيه من قلب الحقائق وظلم للنفس حيث قرن التزوير بالإشراك بالله، ولعظيم هذا الفعل فإنه ﷺ قد غيّر من هيئته بعدما كان متكئا

---

(1) الإحالات في النسخة المنقوحة.

(2) الإحالات في النسخة المطبوعة.

...../...

فجلس لبيان عظيم أهمية هذا التصرف الذي هو الزور، وبقي يكرر كلامه مرارا لخطورة الموضوع الشديدة التي ينبغي تجنبها والحذر منها.

الفرع الثالث: أدلة تحريم التزوير من المعقول

إن الله سبحانه وتعالى قرن بين الزور والإشراك بالله، كما شدد رسول الله ﷺ على فاعله فحرم التزوير لما يلحقه من ضرر جسيم على المُعتدى عليه كما قد يلحق الأذى بالمجتمع كله وهو ما يتنافى ومقاصد الشارع، فلزم أن يحرّم للظلم الذي يلحق بالجميع والظلم منهي عنه في قوله تعالى:﴿ وَمَا ٱللَّهُ يُرِيدُ ظُلْمًا لِّلْعَٰلَمِينَ ﴾ [1]، وقوله عز وجل:﴿ وَمَا رَبُّكَ بِظَلَّٰمٍ لِّلْعَبِيدِ ﴾ [2]. [3]

المطلب الرابع: عقوبة التزوير في الفقه الإسلامي

يخضع المزور في التشريع الجنائي الإسلامي إلى عقوبات تعزيرية وفق ما يقدره الإمام ويراه مناسبا آخذا بعين الاعتبار شخص المزور ومكان التزوير وزمانه، وذلك بغرض زجر المزور وردع غيره عن ارتكاب هذا التصرف المحرم، وقد عرف التزوير أشكالا عدة من العقوبات في التشريع الإسلامي وبيانها في الفروع التالية:

الفرع الأول: التشهير بالمزور

التشهير من الشهرة، ومعناه إظهار الشيء بشكل بشع حتى يعرفه الناس، والشهرة الفضيحة[4]. وقد كان يشهر عقابا بوضع الجاني في مكان مرتفع حتى يعرفه الناس، أو الإعلان عنه في مسجده أو بين أفراد قبيلته أو في بلدته أو الطواف به في الأماكن التي يعرف بها[5]، أما حديثا فالتشهير يتم عن طريق وسائل الإعلام المقروءة أو المسموعة أو المرئية.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني: تسويد الوجه وتسخيمه

السخمة السواد، والأسخم الأسود، وسخم إليه وجهه أي سوده[1].

وهي عقوبة اختلف فيها فقهاء المذاهب الأربعة؛ فلا يقول بها الحنفية باعتبارها من باب المُثلة وقد نهى عنها النبي ﷺ[2]، أما المالكية فيقولون بحلق الرأس عقوبة، وتسويد الوجه يكون معنويا عن طريق التشهير بالجاني[3]، كما حكي بجواز تسويد الوجه حقيقة[4]. أما الشافعية فأجازوا حلق رأس الجاني دون لحيته عقابا وفي تسويد الوجه خلاف في المذهب[5] وللإمام إسقاط هذه العقوبة إذا رأى في ذلك مصلحة. بينما اختلف الحنابلة في تسويد الوجه باعتبار نهيه ﷺ عن المُثلة[6]، على أن للإمام الحق في تقدير العقوبة دون مخالفة النص الشرعي[7].

الفرع الثالث: عدم قبول شهادة المزور في القضاء

اتفق الفقهاء على عدم قبول شهادة المزور في المحاكم ولا أي من الوثائق الرسمية التي يقدمها، إلا أنهم اختلفوا في حالة توبته على قولين، فذهب جمهور الفقهاء (الحنفية، والشافعية، والحنابلة) على أن عقوبة عدم قبول المزور في القضاء تنطبق على إصرار المزور على فعلته وترفع هذه العقوبة في حال توبته وظهور صلاحه[8]، واشترط الحنفية أن يعلن توبته عند القاضي[9]، أما المالكية فيقولون بعدم قبول المزور في القضاء (الشهادة، وتقديم الوثائق الرسمية) وردوا على بعض المالكية الذين أجازوا قبول الجاني إذا تاب وعرف صلاحه، أن التوبة يجب أن تكون قبل الحكم[10].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

هذا وقد اتفق جمهور فقهاء المذاهب الأربعة على من ثبت عليه التزوير يعاقب بالتعزير ويشهر به، والتعزير يكون بالضرب والجلد والحبس والنفي[1]، على أن تعود العقوبة لما يراه الإمام مناسبا حسب الزمان والمكان على أن لا يخالف نصا شرعيا، واشترطوا لتطبيق العقوبة أن لا يزيد عن الحد الأدنى للعقوبات الحدية، وأن يراعى فيه حال المجرم وظروف الجريمة والنتائج المترتبة على جرمه.

المطلب الخامس: حكم التزوير الإلكتروني

لقد حرص التشريع الإسلامي على تجريم كل المخاطر التي تهدد الإنسان والمجتمع، ومن بينها التزوير قولا وفعلا، فقول الزور هو قول كاذب مخالف للحقيقة والقصد منه إيهام الغير باعتقاد أمر على غير الحقيقة لإبطال الحق وإحقاق الباطل، وقد حرّمه المولى سبحانه وتعالى في قوله عز وجل:﴿فَٱجْتَنِبُواْ ٱلرِّجْسَ مِنَ ٱلْأَوْثَٰنِ وَٱجْتَنِبُواْ قَوْلَ ٱلزُّورِ ﴾[2].

وقياسا على ما تم عرضه حول التزوير وأحكامه في الشريعة الإسلامية، باعتباره تمويه الباطل بما يوهم أنه حق[3] ومن فعل ذلك استحق العقوبة التعزيرية، فلا شك أن مزوّر المحررات الإلكترونية ذات القيمة الإثباتية ينطبق عليه تمويه الباطل بما يوهم أنه حق ولذلك فإنه يستوجب العقوبة التعزيرية لما يلحقه من أضرار جسيمة التي من بينها؛ ضياع الحقوق وأكل الأموال بالباطل وتشويه صورة الآخرين والإساءة إلى سمعتهم عن طريق تزوير أقوالهم ومواقفهم، والإخلال بثقة الناس في التعاملات الإلكترونية مما يعيق حياة المجتمعات الحديثة، كما طالت أضراره أيضا التجارة الإلكترونية والحكومات الإلكترونية لما تتعرض له من حالات التزوير الواسعة وغيرها من الخسائر المادية والمعنوية. والزور كما يكون بالقول يكون بالفعل ولذلك فإنه يشمل تزوير المحررات والمستندات والوثائق الإلكترونية، لما في ذلك من إبطال الحق وإثبات الباطل.

كما يشتمل التزوير على الغش الذي حرمته الشريعة الإسلامية وقد نهى عنه النبي ﷺ في قوله: (من غشنا فليس منا)[4] لما فيه من تغيير للحقيقة وخداع لصاحب الحق، وفيه أكل أموال الناس

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

بالباطل والله عز وجل يقول :﴿ وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ وَتُدْلُواْ بِهَآ إِلَى ٱلْحُكَّامِ لِتَأْكُلُواْ فَرِيقًا مِّنْ أَمْوَٰلِ ٱلنَّاسِ بِٱلْإِثْمِ وَأَنتُمْ تَعْلَمُونَ ﴾[1].

وبالإضافة إلى عقوبات التعزير التي تسلط على المزور، فإنه يضمن أيضا ما أخذه من مال أو ما تسبب به من ضياع مال، أو تلف أو ضرر حصل للغير بسبب هذا التزوير، فيعاقب بما يرفع الضرر عن غيره وهو ما ذهب إليه الفقهاء من تضمين شاهد الزور ما ترتب على شهادته من إتلاف لأنه سبب في إتلافه[2].

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الرابع:
جرائم التعدي على النقود الإلكترونية

لقد عرفت النقود تطورا مستمرا سعيا لإحراز قدر أكبر من الكفاءة في أداء وظائفها وفي ضبط التبادل وتيسيره، وشاء الله عز وجل أن تشهد البعثة النبوية الشريفة أهم مرحلة من مراحل تطور النظام النقدي أين سادت فيه النقود المعدنية من الذهب والفضة حيث ورد في شأنهما جملة من الأحكام الشرعية، و لم تتوقف النقود عن التطور بل اتخذت أشكالا متنوعة إلى أن وصلت إلى صورتها المتعارف عليها عالميا من العملات الورقية والمعدنية.

وفي مجال التكنولوجيا الحديثة كان للتجارة الإلكترونية دور هاما في تطوير الحركة المصرفية حيث أصبح بالإمكان إجراء المعاملات المالية من خلال شبكة الانترنت وذلك باستخدام وسائل الدفع الإلكترونية التي تتيحها البنوك والمصارف، وكنتيجة لذلك ظهر شكل جديد من النقود كوسيلة للدفع والإبراء عرف بالنقود الإلكترونية التي سرعان ما انتشرت وأصبحت إحدى أنشطة الخدمات المصرفية التي تقدمها الآلاف من المصارف على المستوى العالمي ويتعامل بها مئات الملايين من الأفراد لسد حاجياتهم من السلع والخدمات، إلا أن هذا النوع من النقود لم يسلم هو أيضا من اعتداءات السرقة والتزوير شأنها شأن النقود التقليدية.

المطلب الأول: مفهوم النقود الإلكترونية

الفرع الأول: تعريف النقود في اللغة

النقد في اللغة يطلق على معان عدة منها؛ التمييز ونقد الدراهم إذا أخرج منها الزيف، ومنها الإعطاء والقبض، ومنها يطلق النقد على قطعة المعدن المضروبة للتعامل بها[1]، ويطلق النقد بمعنى خلاف النسيئة[2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثاني: تعريف النقود اصطلاحا

أولا: النقود في القرآن والسنة:

لم يرد لفظ النقود في القرآن الكريم والسنة الشريفة، إنما ورد ما يستعمل كنقود ولاسيما الذهب والفضة باعتبارهما وسائل دفع تؤدي وظائف النقود وذلك في قوله تعالى:﴿ وَٱلَّذِينَ يَكۡنِزُونَ ٱلذَّهَبَ وَٱلۡفِضَّةَ وَلَا يُنفِقُونَهَا فِي سَبِيلِ ٱللَّهِ ﴾ [1]، فما يقع عليه الإنفاق هو النقود، وقوله تعالى:﴿ وَمِنۡ أَهۡلِ ٱلۡكِتَٰبِ مَنۡ إِن تَأۡمَنۡهُ بِقِنطَارٖ يُؤَدِّهِۦٓ إِلَيۡكَ وَمِنۡهُم مَّنۡ إِن تَأۡمَنۡهُ بِدِينَارٖ لَّا يُؤَدِّهِۦٓ إِلَيۡكَ إِلَّا مَا دُمۡتَ عَلَيۡهِ قَآئِمٗا ﴾[2]، وقوله تعالى: ﴿ وَشَرَوۡهُ بِثَمَنِۭ بَخۡسٖ دَرَٰهِمَ مَعۡدُودَةٖ وَكَانُواْ فِيهِ مِنَ ٱلزَّٰهِدِينَ ﴾[3]، ومن السنة النبوية ما ورد عن عروة البارقي رضي الله عنه: (أن النبي صلى الله عليه وسلم أعطاه دينارا يشتري له شاة، فاشترى له شاتين، فباع إحداهما بدينار، وأتى صلى الله عليه وسلم بدينار وشاة، فدعا له رسول الله صلى الله عليه وسلم بالبركة في بيعه، فكان لو اشترى ترابا لربح فيه)[4]، والدينار والدرهم هما النقود المضروبة من الذهب والفضة، إذ أن الدينار هو وحدة النقود المضروبة من الذهب وهي تعادل مثقال ويساوي 4.25 غ من الذهب، والدرهم هو وحدة النقود المضروبة من الفضة وتزن العشرة دراهم سبعة مثاقيل، وهذه الأوزان لم تتغير في الجاهلية ولا في الإسلام وبهما تقدر الأحكام الشرعية المختلفة[5].

ثانيا: النقود عند الفقهاء

ذهب الفقهاء إلى عدم اقتصار النقود على الذهب والفضة بينما أكدوا على دور العرف في اعتماد النقود، وفي ذلك قول عمر بن الخطاب رضي الله عنه: "هممت أن أجعل الدراهم من جلود الإبل، فقيل له: إذن لا بعير فأمسك"[6] وهو ما يفيد بأن النقد أمر سلطاني خاضع للدولة، ولأن الإبل كانت واسطة للنقل وأداة للجهاد لدى المسلمين امتنع عمر بن الخطاب رضي الله عنه عن ضرب الدراهم منها، وقال الإمام مالك رحمه الله في المدونة: "ولو أن الناس أجازوا بينهم الجلود حتى تكون

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

لها سكة وعين، لكرهتها أن تباع بالذهب والورق نظرةً ـــ أي نسيئةـــ"[1] ومعناه يحرم بيعها نسيئة مخافة الربا لاشتراكها بالعلة الربوية مع الذهب والفضة.

وبناء على ذلك يمكن تصنيف نوعين من النقود في الفقه الإسلامي؛ هي النقود الخلقية والنقود الاصطلاحية، فالأولى تشير إلى النقود المضروبة من الذهب والفضة[2] والتي كانت سائدة زمن نزول التشريع الإسلامي وهي التي قدرت بها الأحكام الشرعية حيث يقول السرخسي بهذا الشأن "الذهب والفضة ثمن بأصل الخلقة، فالتبر والمضروب في كونه ثمنا سواء"[3]، وقال ابن عابدين "ولاشك أن الجياد لا تبطل ثمنيتها بالكساد لأن ثمنيتها بأصل الخلقة كما صرحوا به لا بالاصطلاح"[4] والمقصود من ذلك أن الذهب والفضة أثمان بأصل الخلقة فالقوة الشرائية لهما مستمدة من طبيعتهما المعدنية التي تضفي عليهما قيمة سلعية تتحدد بفعل قوى السوق الممثلة في العرض والطلب.

أما النقود الاصطلاحية فهي النقود التي تعارف الناس على استخدامها بحكم العرف أو القانون الذي يلزم الناس بها، وهي تشمل الدراهم والدنانير والفلوس الرائجة، والأوراق النقدية والبطاقات البلاستيكية، والنقود الإلكترونية، فهي كالنقود التي همّ عمر بن الخطاب رضي الله عنه اتخاذها من جلود الإبل، وهي ذاتها التي أجرى فيها حكم الربا الإمام مالك رحمه الله.

الفرع الثالث: تعريف النقود الإلكترونية

نظرا لحداثة هذا النوع من النقود فإنها تعرف مسميات عدة للتعبير عنها، كالنقود الرقمية Digital money، أو العملة الرقمية Digital Currency، أو النقدية الإلكترونية Electronic Cash وكلها تعبر عن مفهوم واحد هو التعامل الإلكتروني، وقد عرف هذا النوع من النقود تعريفات عديدة من أهمها تعريف المفوضية الأوربية بأنها:" قيمة نقدية مخزنة بطريقة إلكترونية على وسيلة إلكترونية كبطاقة أو ذاكرة كمبيوتر، ومقبولة كوسيلة للدفع بواسطة متعهدين غير المؤسسة التي أصدرتها، ويتم وضعها في متناول المستخدمين لاستعمالها كبديل عن العملات النقدية والورقية، وذلك بهـــدف

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

إجراء تحويلات إلكترونية لمدفوعات ذات قيمة محددة" [1].

وعرّفها البنك الدولي على أنها: " قيمة نقدية في شكل وحدات ائتمانية مخزونة بشكل الكتروني على أداة الكترونية يحوزها المستهلك "[2] ، وعرفها البنك الأوربي بأنها: " مخزون الكتروني لقيمة نقدية على وسيلة تقنية يستخدم بصورة شائعة للقيام بمدفوعات لمتعهدين غير من أصدرها دون الحاجة إلى وجود حساب بنكي عند إجراء الصفقة وتستخدم كأداة مدفوعة مقدما"[3].

كما تعرّف بأنها "عملة نقدية إلكترونية تتمثل في الوحدات الرقمية الموثقة والخاصة بالقيمة المحددة من قبل الجهة المصدرة لها، والمخزنة على أداة أو وسيلة الكترونية ليتم تحويلها من المشتري إلى البائع أو إلا أي جهة أخرى"[4]. وتعرّف أيضا بأنها "مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية أن تحل فعليا محل تبادل العملات التقليدية"[5].

وما يمكن استخلاصه من هذه التعريفات أن النقود الإلكترونية عبارة عن وحدات نقدية ذات قيمة مالية مخزنة على وسائط إلكترونية، وتحظى بقبول واسع من قبل الأشخاص والمؤسسات كوسيلة للدفع بغرض تحقيق منافع مختلفة، بمعنى أن النقود الإلكترونية هي المكافئ الإلكتروني للنقود التقليدية التي اعتاد الناس تداولها.

الفرع الرابع: أنواع النقود الإلكترونية

تتخذ النقود الإلكترونية أنواعا عدة، ومن أهمها:

1 ـــ البطاقات البلاستيكية الممغنطة: هي بطاقات تصدرها البنوك للتعامل بها بدلا من حمل النقود ومن أشهرها تداولا بطاقة الفيزا Visa Card ، والماستر كارت Master Card، وهي بطاقات تمثل قيمة من المال مدفوعة سلفا ومخزنة فيها، حيـــث تتيح إمكانية الدفع عبر الانترنت وغيرهـــا من الشبكات كما يمكن استخدامها للدفع في نقاط البيع التقليدية كالمحلات ومحطات البترين وغيرها.[6]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وبالإضافة إلى ذلك هناك أنظمة برمجية تتيح مكافئا إلكترونيا دون الحاجة إلى البطاقة البلاستيكية وهي عبارة عن برامج مخصصة لدفع النقود عبر الانترنت يشرف عليها بنك يعمل إلكترونيا عبر الانترنت Online Bank ، حيث يتيح هذا البنك برنامجا نقديا للإيفاء يوفره للمتعاملين المرتبطين بمنفذ الانترنت، ومن أشهر هذه البرامج E. Cash الذي يستخدم لإتمام عمليات الشراء والدفع عبر الانترنت [1].

2 ـــ المحفظة الإلكترونية Electronic Wallet :

يتم في هذا النوع من النقود تخصيص مبالغ مالية إما في بطاقة ذكية مزودة بشريحة الكترونية قادرة على تخزين بيانات تعادل 500 ضعف ما يمكن تخزينه على البطاقات البلاستيكية الممغنطة لكن تنتهي صلاحيتها مباشرة بعد نفاذ المبالغ المحملة عليها، وإما تخصيص مبالغ محددة تثبّت على ذاكرة كمبيوتر الجهة التي تقدم خدمة الدفع الإلكتروني حيث يقوم العميل بالحصول على وحدات النقد الإلكتروني من البنك حسب الكمية المرغوب فيها على شكل وحدات نقد صغيرة ويطلب وضعها في محفظة النقود التي يختارها، ويتم الوفاء من المشتري إلى البائع عن طريق برنامج خاص بإدارة الدفع الإلكتروني يستوجب توفره لدى الطرفين[2].

3 ـــ النقود الائتمانية الإلكترونية:

وتعرف بالنقود الرقمية أو الرمزية حيث تسجل قيمة العملة الموثقة على وسائط إلكترونية تسمى ببطاقات الائتمان، وهي بطاقات يمنحها البنك لحاملها كتسهيلا ائتمانيا تمكنه من استعمالها في المعاملات المالية ويتولى البنك السداد، ثم يقوم حاملها بتسديد ما دفعه البنك خلال أجل متفق عليه ووفق شروط معينة ـــ مع وجوب مراعاة الضوابط الشرعية في بلاد الإسلام ـــ، وهذا النوع من النقود يسمح بالوفاء مباشرة بالمقابل النقدي للعقد الإلكتروني عن طريق الانترنت دون الحاجـــة إلى الاتصال بالمتعاقد أو تدخل أي وسيط[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

4 ــ الصكوك الإلكترونية Electronic Checks :

تكافئ الصكوك الإلكترونية الصكوك الورقية التي اعتاد الناس بالتعامل بها، والصك الإلكتروني عبارة عن وثيقة الكترونية موثقة ومؤمنة يتعهد فيها البنك بسدادها وفق شروط معينة، وهي تحتوى على البيانات التالية: رقم الصك، واسم صاحبه ورقم حسابه، واسم المصرف، واسم المستفيد والقيمة التي ستدفع، ووحدة العملة المستعملة، وتاريخ الصلاحية، والتوقيع الإلكتروني. يقوم مصدر الصك بإرساله عن طريق الانترنت إلى مستلمه (حامله) ليعتمده ويقدمه للمصرف الذي يعمل عبر الانترنت أيضا، فيقوم المصرف بتحويل القيمة المالية للصك إلى حساب حامله ثم يخطر كل من الطرفين بتمام إجراء المعاملة المصرفية[1].

المطلب الثاني: مدى مشروعية النقود الإلكترونية وحكم التعدي عليها

الفرع الأول: مشروعية النقود الإلكترونية

لم يرد نص شرعي يفيد الالتزام باستعمال نوع معين من النقود أو يحرّم نوع آخر، ولذلك فإن استخدام النقود المعدنية أو الورقية أو المصرفية وكذا النقود الإلكترونية بما يتلائم وظروف كل عصر إنما هو من باب ما تقتضيه مصلحة الأمة، ولما كانت الشريعة الإسلامية مبنية على الحكم والمصالح كما أشار إلى ذلك فقهاء الشريعة، فإن مبنى استخدام النقود الإلكترونية هو تحقيق مصالح المتبايعين عن بعد مهما كان موقعهما وبالتالي تيسر عملية المبادلة وتحقق مصالح الناس لاسيما في ظل الثورة المعلوماتية. كما تساند القواعد الفقهية مشروعية النقود الإلكترونية في قاعدة "الأمور بمقاصدها"؛ فالمقصود من النقود أنها وسيلة للمبادلة، ولما كانت النقود الإلكترونية تؤدي هذا المقصد فهي تعد من النقود المقبولة شرعا، وما يدل أيضا على مشروعيتها قاعدة "ما لا يتم الواجب إلا به فهو واجب" ولما كانت التجارة الإلكترونية هي السائدة حاليا فإن ذلك يقتضي وجود النقود الإلكترونية لتسهيل إبرام العقود وإلا وقعت الأمة في حرج وتعطل الواجب، وبما أن القيمة المخزنة على الوسائط الإلكترونية تمثل وحدات نقدية حازت على القبول العام وحصول الثقة بها كوسيط في التداول

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والتبادل، فهي إذا نقد في حكم النقود الورقية وبديل عنها[1].

الفرع الثاني: حكم التعدي على النقود الإلكترونية

ما دامت النقود الإلكترونية من الأموال المتقومة فإنه يحرم التعدي عليها، لأن المال من الكليات الخمس التي أمرت الشريعة الإسلامية بالمحافظة عليه وذلك في قوله تعالى:﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَأۡكُلُوٓاْ أَمۡوَٰلَكُم بَيۡنَكُم بِٱلۡبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٖ مِّنكُمۡۚ ﴾ [2]، وقال ﷺ: (إن الله حرم عليكم دماءكم وأموالكم كحرمة يومكم هذا ، في بلدكم هذا في شهركم هذا ، ألا هل بلغت ؟ قالوا : نعم ، قال : اللهم اشهد)[3]، وقال ﷺ فيما روته عائشة رضي الله عنها: (تقطع اليد في ربع دينار فصاعدا)[4].

والسؤال المطروح هل سرقة النقود الإلكترونية توجب الحد خاصة وأن وسائطها تتنوع من بطاقات ذكية وصكوك إلكترونية وأرصدة بالبنوك والمصارف الإلكترونية وغيرها، علما أن الشريعة الإسلامية حددت شروط إقامة حد السرقة كما يلي:

أولاً : أن يكون الجاني مكلفا، وأن يقصد فعل السرقة دون الاضطرار إلى الأخذ، وأن لا تقترن أي شبهة في استحقاقه لما أخذ[5].

ثانياً : أن يكون صاحب المال معلوما وأن يكون معصوم المال، حيث ذهب الجمهور إلى درء الحد عن السارق إذا كان المسروق منه مجهولاً، كأن تثبت السرقة و لم يعرف من هو الضحية لأن إقامة الحد تتوقف على دعوى المالك أو من في حكمه، ولا تتحقق الدعوى مع الجهالة[6]، وذهب

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المالكية إلى إقامة الحد على السارق متى ثبتت السرقة دون تفريق بين ما إذا كان الضحية معلوما أو مجهولاً لأن إقامة الحد عندهم لا تتوقف على دعوى المالك[1].

ثالثاً : أن يكون المال المسروق متقوما شرعا لأن سرقة ما لا قيمة له في نظر الشرع لا حد له، وأن يبلغ النصاب على اختلاف بين الفقهاء في مقدار النصاب[2]، وأن يكون محرزاً[3] بحيث لا يعد صاحبه مضيعاً له بوضعه فيه، فقد ذهب جمهور الفقهاء إلى أن حد السرقة لا يقام إلا إذا أخذ السارق النصاب من حرزه لأن المال غير المحرز ضائع بتقصير صاحبه في حفظه[4]، وفي ذلك قال النبي ﷺ: (ما أخذ في غير أكمامه فاحتمل ففيه قيمته ومثله معه، وما كان في الجرين ففيه القطع إذا بلغ ثمن المجن)[5]، وكما سبق ذكره فإن ضابط الحرز وتحديد مفهومه مرده إلى العرف، وهو يختلف باختلاف الزمان والمكان ونوع المال المحفوظ.

رابعاً : يشترط لإقامة حد السرقة أن يؤخذ الشيء المسروق خفية واستتاراً بأن يكون ذلك دون علم المأخوذ منه ودون رضاه، أما إذا أخذ الشيء مجاهرة فإن هذا الفعل لا يسمى سرقة وإنما هو مغالبة أو نهباً أو اغتصاباً[6]، وفي ذلك قوله ﷺ: (ليس على الخائن ولا المختلس قطع)[7]، كما يشترط أن يخرج المسروق من الحرز بعد هتكه سواء أخرجه بنفسه أو باستعمال وسيلة ما.

ولذلك فإن جمهور الفقهاء يمنعون إقامة الحد إذا لم تتم شروط السرقة لكن يوجبون التعزير في كل من يشرع في السرقة[8].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وبالرغم من اتفاق نتائج جريمة السرقة الإلكترونية مع جريمة السرقة التقليدية إلا أن هناك أمور تستوجب البحث لما لها من أثر في تسليط الحكم الشرعي خاصة فيما يتعلق بالحرز وذلك بالنظر إلى مدى الضمانات الفنية والحماية الأمنية للتعاملات الإلكترونية، حيث كلما قويت أنظمة الحماية الأمنية دلت على وجود الحرز الذي هو شرط من شروط اكتمال جريمة السرقة، ومما يؤثر في الحكم أيضاً عدم مطالبة مالك المال المسروق بماله وذلك بسبب ما قد يترتب عليه من إساءة للسمعة وفقدان ثقة الغير من التعامل معه[1].

وما يمكن تسجيله فيما يخص التعدي على النقود الإلكترونية إضافة إلى المجاهرة والمغالبة، أن الكثير من الاعتداءات التي تطال المال الإلكتروني تصدر عن منظمات إجرامية تهدد أمن واستقرار واقتصاد المجتمع، الأمر الذي دعا بعض العلماء المعاصرين إلى إدراج هذا النوع من الجرائم ضمن الحرابة والإفساد في الأرض، فإذا كان الجاني ذا شوكة وقوة وتنظيم وقام بنهب الأموال، فإنه يطبق عليه حد الحرابة[2].

ومعنى ذلك لو كان الغاصب يعمل ضمن عصابة للاعتداء والسطو فهذا يأخذ حكما مغايرا لحكم السرقة، نظرا لعظم الجرم وخطورته على أمن الأفراد والمجتمع فكان لزاما أن يكون التوصيف الشرعي مناسبا للاعتداء، ولعل أقرب الجرائم المشخصة لهذا الفعل الخطير هي جريمة الحرابة، وهي جريمة لا يستطيع فيها المجني عليه الدفاع عن نفسه أو الاستغاثة بغيره نظرا لقوة التدبير المحكم وهو حال الكثير من الجرائم الإلكترونية[3].

والحرابة اصطلاحا هي قيام طائفة مسلحة بإحداث الفوضى أو القتل أوالنهب والسلب أو الإرهاب أو هتك الأعراض اعتمادًا على القوة، وتُعْرف الحرابة أيضًا بـــ قطع الطريق[4]، وقد اتفق الفقهاء في بيان حد الحرابة مما ورد في قوله تعالى:﴿ إِنَّمَا جَزَٰٓؤُاْ ٱلَّذِينَ يُحَارِبُونَ ٱللَّهَ وَرَسُولَهُۥ وَيَسۡعَوۡنَ فِي ٱلۡأَرۡضِ فَسَادًا أَن يُقَتَّلُوٓاْ أَوۡ يُصَلَّبُوٓاْ أَوۡ تُقَطَّعَ أَيۡدِيهِمۡ وَأَرۡجُلُهُم مِّنۡ خِلَٰفٍ أَوۡ يُنفَوۡاْ مِنَ ٱلۡأَرۡضِۚ ذَٰلِكَ لَهُمۡ خِزۡيٞ فِي

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ٱلدُّنۡيَاۖ وَلَهُمۡ فِي ٱلۡأٓخِرَةِ عَذَابٌ عَظِيمٌ ﴾ [1].

واختلف الفقهاء في الحكم الوارد في الآية من حيث تخيير الإمام في تحديد عقوبة الحرابة بناءً على الآية، ومنهم من يقول بوجوب تحديد العقوبة بناءً على الآية على سبيل الترتيب لا التخيير، فيكون حد الحرابة مبنيًا على نوع الجريمة التي ارتكبها ذلك المجرم، بحيث يكون الترتيب على النحو التالي[2]:

ـــ فإذا قتل وأخذ مالا، كانت عقوبته القتل والصلب، ولا يعفى عنه.

ـــ أما إذا قتل و لم يأخذ مالا قُتِل من دون صَلبٍ.

ـــ وإذا أخذ مالا من دون قتل، كانت عقوبته قطع اليد اليمنى والرجل اليسرى.

ـــ أما من أرهب الناس وأخافهم من دون قتل أو سلب للأموال، كانت عقوبته النفي من الأرض والتشريد.

وبالنظر إلى الخلاف القائم في أقوال الفقهاء في المسألة، فإن التعزير هو الأقرب للصواب خاصة وأن حد السرقة أدنى من الحرابة ولئن يخطئ الإمام في العفو خير من أن يخطئ في العقوبة كما جاء في حديث رسول الله صلى الله عليه وسلم عن عائشة رضي الله عنها قالت: (قال رسول الله صلى الله عليه وسلم ادرءوا الحدود عن المسلمين ما استطعتم فإن كان له مخرج فخلوا سبيله فإن الإمام أن يخطئ في العفو خير من أن يخطئ في العقوبة) [3].

ونتيجة المسألة أن سرقة النقود الإلكترونية محرّم ويستوجب الحد إذا توفرت شروط السرقة خاصة ما يتعلق بانتهاك الحرز الإلكتروني وتبليغ الضحية، كما لن يسلم السارق من عقوبة التعزير في حال قيام شبهة السرقة وذلك وفق ما يقرره الحاكم ويراه مناسبا مقارنة بما تلحقه سرقة المال الإلكتروني من أضرار وحسب ما تقتضيه الظروف.

---

(1) الإحالات في النسخة المعتمدة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الخامس:
جرائم التعدي على التجارة الإلكترونية

المطلب الأول: مفهوم التجارة الإلكترونية وفوائدها.

الفرع الأول: تعريف التجارة الإلكترونية

لقد عرفت التجارة الإلكترونية E-Commerce عدة وجهات نظر في تعريفها نذكر منها على سبيل المثال لا الحصر[1]:

تعرّفها منظمة التجارة العالمية بأنها: مجموعة متكاملة من عمليات عقد الصفقات وتأسيس الروابط التجارية وتوزيع وتسويق وبيع المنتجات بوسائل إلكترونية.

كما تعرّف بأنها تنفيذ بعض أو كل العمليات التجارية في السلع والخدمات عبر شبكة الانترنت والشبكات العالمية الأخرى، أي باستخدام تكنولوجيا المعلومات والاتصالات، وهي وسيلة سهلة وسريعة لإبرام الصفقات التجارية إلكترونيا سواء كانت التجارة في السلع والخدمات، أو المعلومات.

وتعرّف أيضا بأنها مجموعة العمليات التجارية التي تتم بين طرفين أو أكثر باستخدام أجهزة الكمبيوتر المتصلة عبر شبكات الاتصال؛ والعمليات التجارية هي تعاملات البيع والشراء بين البائع والمشتري، وتعاملات بينية في قطاعات الأعمال، والتسوق الإلكتروني، والتعاملات المصرفية، كما تقوم التجارة الإلكترونية بوظائف أخرى كالإعلان وإصدار الفواتير الإلكترونية وتوفير الدعم الفني إلكترونيا للعملاء وغيره.

كما تعرّف التجارة الإلكترونية بأنها تنفيذ عمليات شراء وبيع البضائع والخدمات والمعلومات عبر شبكات الاتصالات والمعلومات ويشمل ذلك الإعلان عن تسويق وبيع السلع والبضائع والخدمات ودعم الشراء والبيع وخدمات ما بعد البيع.

وما يجب معرفته أن التجارة الإلكترونية أكبر بكثير من مجرد موقع على شبكة الانترنت، بحيث تتعدد مستوياتها تبعا لمدى تنفيذ الأنشطة الفرعية المرتبطة بأداء التعاملات التجارية، فتتراوح بين

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المستوى البسيط الذي يشمل الترويج والدعاية والخدمات وتوزيع السلع والتحويلات البسيطة، والمستوى الأكثر تطورا الذي يتضمن التوزيع والدفع على المستوى المحلي والعالمي[1].

الفرع الثاني: فوائد التجارة الإلكترونية

تسمح التجارة الإلكترونية بترشيد قرارات كل من البائعين والمشترين بما تتميز به من تدفق المعلومات في الوقت المناسب وبطريقة منسقة ودقيقة، وهو ما يسمح بتيسير المقارنة بين المنتجات من ناحية الأسعار أو الجودة أو طريقة الدفع والتسهيلات، ولقد أصبحت في عصرنا ذات أهمية بالغة بالنسبة للمنتجين والمستهلكين والمجتمع ككل نظرا لتغلبها على حواجز المسافة واختلافات التوقيت ونقص المعلومات، ومن فوائدها ما يلي:

أولا ـــ فوائد التجارة الإلكترونية بالنسبة للمجتمع:

تعتبر التجارة الإلكترونية أداة لرفع القدرة التنافسية وزيادة الصادرات نتيجة سهولة الوصول إلى مراكز الاستهلاك وإمكانات تسويق السلع والخدمات عالميا، وسرعة عقد وإنهاء الصفقات، وتحليل الأسواق والاستجابة لتغيرات احتياجات ومتطلبات المستهلكين، كما تحقق للمشروعات المشاركة في التجارة العالمية وتوفر لها قدرة الوصول إلى الأسواق العالمية، وتتيح للمنتج القيام بمعاملات تجارية في دول العالم بفاعلية وكفاءة عن طريق خفض تكاليف التسويق والدعاية والإعلان وتوفير الوقت وهو ما ينعكس إيجابا على تنشيط المشروعات.

كما تخلق التجارة الإلكترونية فرص العمل الحر والعمل في المشروعات الصغيرة والمتوسطة التي تتصل بالأسواق العالمية بأقل تكلفة استثمارية حيث تمثل تجارة الخدمات مجالا أساسيا في التجارة الإلكترونية، وهي تعتبر أداة لزيادة شفافية الأعمال الحكومية وتحسين الخدمات وتبسيط الإجراءات وتسهيل المعاملات الحكومية وتحقيق التواصل مع المواطنين نظرا لتيسير هذه الأداة في توزيع الخدمات العامة مثل الصحة والتعليم والخدمات الاجتماعية بكفاءة أعلى، كما تساهم التجارة الإلكترونية في زيادة الاستثمار بتوفير المعلومات للمستثمرين ورجال الأعمال وعرض إجراءات وخطوات ونماذج الخدمات الحكومية وأداء الخدمات إلكترونيا، كما تسمح بالتواصل والاستفادة من فرص التكنولوجيا المتقدمة بخلق مناخ لدخول شركات وأعمال جديدة في مجال التكنولوجيا المتطورة وأعمال البنية

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الأساسية لنظم المعلومات والاتصالات، كما تساهم في رفع مستوى معيشة ذوي الدخل المحدود بالنظر إلى ما تتيحه من تنوع في السلع والخدمات بأسعار زهيدة حيث يتمكن الأفراد والمجتمعات من إشباع حاجاتهم من السلع والخدمات المعروضة على المستوى العالمي[1].

ثانيا ـــ فوائد التجارة الإلكترونية بالنسبة للشركات والمؤسسات:

يمكن تلخيص فوائد التجارة الإلكترونية في تحقيق عائدات وخفض تكاليف العمالة وسرعة الوصول إلى المعلومات وخفض تكاليف المخازن، وتقديم الخدمات للعملاء على مدار الوقت، وسرعة نشر المعلومات وتوزيعها، وخفض تكاليف الاتصالات، وسهولة جمع المعلومات.

ويساهم اعتماد الشركات على الانترنت في عرض وتسويق منتجاتها وخدماتها في العالم دون انقطاع إلى تحقيق فرصة أكبر لجني الأرباح بسبب الوصول إلى عدد أكبر من العملاء، كما يعتبر إعداد وصيانة مواقع تجارية على الويب أكثر اقتصادا من بناء أسواق التجزئة وتجهيز المكاتب، فهي طريقة لا تحتاج إلى الإنفاق الكبير على أمور الترويج واليد العاملة، إضافة إلى انخفاض تكاليف الاتصالات السلكية واللاسلكية مقارنة بالاتصال عن طريق الانترنت إضافة إلى انخفاض تكاليف التبادل التجاري والتكاليف الإدارية.

كما تعمل التجارة الإلكترونية على إلغاء المسافات والحدود والاستفادة من بضائع وخدمات الشركات الأخرى وإيجاد شركاء تجاريين جدد وتسهيل العمليات التعاقدية، وتوسيع نطاق السوق، وتحسين صورة الشركة وتحسين خدمة الزبائن، وزيادة المرونة في التعامل، واختصار الدورة التجارية وتوفير السرعة في تلبية احتياجات المستهلكين، وتحسين مستوى المنتج وتوفير خدمات ما قبل وبعد البيع، وتوفير معلومات المنتجات والأسواق والاستجابة السريعة لطلبات السوق والمنافسة، كما تعمل على إنشاء تجارة متخصصة وتحقيق فرص عمل جديدة وخدمات ومنتجات جديدة أيضا[2].

ثالثا ـــ فوائد التجارة الإلكترونية بالنسبة للمستهلكين:

توفر التجارة الإلكترونية على المستهلكين الوقت والجهد والقرب؛ حيث لا تعرف الأسواق الإلكترونية التوقف أو العُطل ولا يحتاج الوصول إليها إلى السفر أو الانتظار، كما يتم التسوق وإنهاء

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المعاملات على مدار اليوم والسنة من أي مكان في العالم، ولا يتطلب شراء منتج أكثر من تحديده وإدخال المعلومات عن وسيلة الدفع الملائمة، كما توفر التجارة الإلكترونية فرصة زيارة مختلف أنواع محلات الانترنت وتزود الزبائن بكامل معلومات المنتجات بدون ضغوط الباعة وإحراجهم، إضافة لما تتيحه الانترنت من توفير الكثير من التكاليف المنفقة على الأسواق التقليدية فإن ذلك ينعكس على أسعار السلع بالانخفاض في الأسواق الافتراضية وهو ما يصب في مصلحة المستهلكين[1].

ورغم ما تمتاز به التجارة الإلكترونية من إيجابيات، إلا أنها غدت مرتعا للكثير من الاعتداءات والانتهاكات وبات توفير الحماية الجنائية لها أمرا يفرضه الواقع والمستقبل على حد سواء، فبالإضافة إلى الجرائم الإلكترونية التي تطالها كتغيير محتويات المواقع التجارية وإغلاقها أمام المتصفحين أو تخريبها واختراق أنظمتها الداخلية، فقد عرفت أيضا صور أخرى من الجرائم كان لها أثر سلبيا على موثوقية التجارة الإلكترونية وفي الغالب يكون المستهلك هو ضحيتها الأول، ومن أبرز هذه الصور جريمة الإعلانات التجارية الكاذبة التي أبينها في المطلب التالي.

المطلب الثاني: الإعلانات التجارية الكاذبة

تتميز الإعلانات التجارية بأهمية بالغة في دفع عجلة التقدم الاقتصادي في مختلف القطاعات الإنتاجية، كما تعد موردا هاما لاستمرار عمل الكثير من المؤسسات الحساسة خاصة الإعلامية منها وشركات الدعاية والإعلان، وتساهم الإعلانات بشكل مباشر في ترويج المنتجات السلعية والخدمية مما ينعكس على ترشيد وتغيير أنماط الاستهلاك لدى المتلقين، ولقد أثبتت الإعلانات التجارية مدى تأثيرها على القيم الاجتماعية والتربوية والأخلاقية والثقافية للأمم عن طريق ما تروجه من إيحاءات ورموز قد تكون إما إيجابية أو سلبية[2].

وعلى ضوء ذلك فإن الإعلان الإلكتروني يعتبر من أكثر وسائل الترويج جاذبية وانتشارا في مجال التسويق الإلكتروني، وهو ما تؤكده العديد من الدراسات المهتمة بالإعلان عبر الانترنت بأن

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

معدلات انتشاره تزداد سنويا الأمر الذي يفسر نجاح هذا النوع من التجارة في العالم الافتراضي[1]. لكن بالرغم من أن الإعلان يشكل وسيلة تساعد المستهلك على الاستعلام والاختيار بين السلع والخدمات المعروضة، فإنه قد يكون مصدر خطر إذا بني على الخداع في إيصال المعلومة إلى المستهلك وهو ما أثر بدوره على موثوقية التجارة الإلكترونية.

الفرع الأول: مفهوم الإعلان لغة واصطلاحا

أولا ــ تعريف الإعلان في اللغة:

الإعلان في اللغة يعني الظهور والجهر وهما نقيض السر والكتمان، كما يفيد أحيانا معنى الشيوع والانتشار حيث جاء في لسان العرب: "العلان والمعالنة والإعلان: المجاهرة"[2]. ويقصد به أيضا الذيوع والانتشار " علن الأمر يعلن علونا، وعلن يعلن علنًا وعلانية: إذا شاع وظهر، وعلن الأمر علونا: ظهر وانتشر"[3].

وقد ذكر القرآن الكريم مادة علن ومشتقاتها في كثير من المواضع كانت كلها تفيد معنى البروز والظهور والشيوع، منها قوله تعالى:﴿ رَبَّنَآ إِنَّكَ تَعْلَمُ مَا نُخْفِي وَمَا نُعْلِنُ ﴾[4]، وقوله عز وجل:﴿ وَٱللَّهُ يَعْلَمُ مَا تُسِرُّونَ وَمَا تُعْلِنُونَ ﴾[5].

ثانيا ــ التعريف الاصطلاحي للإعلان:

يتفق المعنى الاصطلاحي للإعلان مع اللغويين على أنه؛ الجهر والإظهار والاشتهار والشيوع ونحوه[6]، حيث جاء في كتاب بداية المجتهد ونهاية المقتصد: "... وأب حنيفة ينعقد النكاح عنده بشهادة فاسقين؛ لأن المقصود عنده بالشهادة هو الإعلان فقط، والشافعي يرى أن الشهادة تتضمن المعنيين: أعني الإعلان والقبول، ولذلك اشترك فيها العدالة، وأما مالك فليس تتضمن عنده الإعلان إذا وصى الشاهدان بالكتمان..."[7]، وجاء في كتاب المغني على مختصر الخرقي ما نصه: " مسألة: قال

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

" إذا تزوجها على صداقين سِر وعلانيةٍ أخذ بالعلانية، وإن كان السر قد انعقد به النكاح"[1].

الفرع الثاني: مفهوم الإعلان التجاري في الاقتصاد الوضعي والإسلامي:

أولا ــ الإعلان التجاري في الاقتصادي الوضعي:

تختلف تعريفات الإعلان التجاري في الاقتصاد الوضعي وفق اعتبارات عدة؛ كاعتباره وسيلة إشهارية وترويجية، أو اعتباره عملية اتصال، أو عملية اقتصادية واجتماعية وغيرها[2]، ومن بين هذه التعريفات: الإعلان التجاري هو عملية اتصال تهدف إلى التأثير من البائع إلى المشتري على أساس غير شخصي، يفصح المعلن عن شخصيته ويتم الاتصال من خلال وسائل الاتصال العامة[3].

كما يعرّف بأنه: نشر بيانات ومعلومات عن السلع والخدمات والأفكار في وسائل النشر المختلفة بقصد بيعها أو المساعدة على بيعها نظير مقابل معين[4].

ثانيا ــ الإعلان التجاري في الاقتصاد الإسلامي:

اتسم مفهوم الإعلان في الاقتصاد الإسلامي ببعض القيود والضوابط التي من شأنها أن يكتسب الإعلان التجاري صفة المشروعية الإسلامية، ومن أبرز التعريفات المتعلقة بهذا المجال أنه: " وصف سلعة أو منفعة مباحة بأسلوب مباح بغرض ترويجها بوسائل نشر عامة، وذلك نظير مبلغ معين يدفعه المعلن"[5]، وهو تعريف يشير إلى أن الإعلان التجاري في الاقتصاد الإسلامي يقوم على أساس الصدق في وصف السلعة أو الخدمة الموجهة للمستهلكين بعيدا عن الأساليب الدعائية المبنية على الكذب والخداع والغش التي من شأنها السيطرة على إرادة المستهلك من خلال المبالغة والتضليل.

والإباحة في التعريف هي قيد يستبعد كل إعلان يروج للسلع المحرمة شرعا، كما يستبعد أيضا كل إعلان لم يلتزم بالضوابط الشرعية في تصميمه ونشره كالإعلانات التي يكشف فيها عن عورات الناس لترويج سلع أو خدمات معينة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثالث: أقسام الإعلان التجاري وأنواعه.

ينقسم الإعلان التجاري وفق اعتبارات عدة أهمها:

1 ــ الإعلان التجاري باعتبار الجمهور المعلن إليه، ومن أنواعه: الإعلان الاستهلاكي الذي يستهدف المستهلك أو خدمة معينة[1]، والإعلان الصناعي وهو موجه بصفة عامة إلى المشترين الصناعيين من الشركات والمنتجين ويتعلق بعرض السلع الصناعية الموجهة للأغراض الإنتاجية[2]، والإعلان المهني وهو نوع يتعلق بتزويد أصحاب المهن بمعلومات عن مستجدات السلع التي يوصون عملائهم بشرائها كالإعلانات المتعلقة بالأدوية التي توجه للأطباء حتى يوصوا المرضى باستخدامها[3].

2 ــ الإعلان التجاري باعتبار الغاية، ومن أنواعه: الإعلان الأولي وهو يهدف إلى ترويج مفهوم سلعي معين بغض النظر عن الأسماء التجارية المختلفة كالإعلانات التي تحث على استهلاك مادة العسل عن طريق توضيح فوائده[4]، والإعلان الاختياري الذي هدفه الترويج عن اسم تجاري معين بقصد استمالة الطلب إليه بدلا من الأسماء التجارية المنافسة[5]، والإعلان عن الاسم التجاري وهدفه الترويج عن اسم شركة أو مؤسسة ما ومدى إسهاماتها في خدمة المجتمع الذي تعمل فيه[6].

3 ــ الإعلان التجاري باعتبار المنطقة الجغرافية، ومن أنواعه: الإعلان الدولي أو العالمي الذي يهدف في الغالب إلى ترويج سلع الدول المتقدمة بغرض التشجيع على تصديرها إلى دول أخرى[7]، والإعلان القومي وهو إعلان يقتصر على جمهور المستهلكين الذين يقيمون في بلد واحد[8]، والإعلان المحلي الذي يقتصر على المستهلكين المقيمين في منطقة جغرافية محددة[9].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الرابع: مشروعية الإعلان التجاري

ذهب العلماء المعاصرون إلى مشروعية الإعلان التجاري باعتبار الأصل إذا كان ملتزما بالضوابط الشرعية، لأن الإعلان ما هو إلا معاملة تجارية مستقلة وما دام كذلك فإن الأصل فيه الإباحة إلحاقا بالمعاملات المالية التي أصلها الجواز، ولقد استدل الباحثون على مشروعية الإعلان التجاري بأدلة عدة أذكر منها على سبيل المثال:

أولا ـــ قوله تعالى على لسان سيدنا يوسف عليه السلام للملك: ﴿ قَالَ ٱجۡعَلۡنِي عَلَىٰ خَزَآئِنِ ٱلۡأَرۡضِۖ إِنِّي حَفِيظٌ عَلِيمٞ﴾ [1]. ووجه الاستدلال من الآية أنه يجوز للإنسان أن يذكر ما فيه من مزايا حميدة كالعلم والفضل وغيرهما إذا دعت الحاجة إلى ذلك لأن الأصل في مدح النفس هو المنع[2] حيث قال تعالى: ﴿ فَلَا تُزَكُّوٓاْ أَنفُسَكُمۡۖ هُوَ أَعۡلَمُ بِمَنِ ٱتَّقَىٰٓ﴾[3]، ولذلك فإنه من باب أولى جواز مدح السلعة والثناء عليها بذكر خصائصها ومنافعها لعدم وجود دليل يمنع ذلك كما هو الشأن بالنسبة لمدح النفس.

ثانيا ـــ لم يؤثر عن النبي ﷺ أنه أنكر على التجار الذين كانوا يعرضون بضائعهم في سوق المدينة المنورة، وينادون عليها إما بأنفسهم أو عن طريق غيرهم للفت أنظار المستهلكين إليها، وهو إقرار منه للمناداة على السلع في الأسواق وهي صورة من الصور البدائية للإعلان التجاري[4].

كما لم يتلق تجار المسلمين إنكارا من أحد حول مناداتهم على السلع في الأسواق للفت أنظار المستهلكين، مما يشير إلى جواز هذه المناداة وهي أحد صور الإعلان[5].

ثالثا ـــ ما صح من حديث أبي هريرة، أن النبي ﷺ مر على صبرة طعام فأدخل يده الشريفة فيها فنالت أصابعه بللا فقال: ما هذا يا صاحب الطعام؟ قال: أصابته السماء يا رسول الله، فقال عليه الصلاة والسلام: (أفلا جعلته فوق الطعام حتى يراه الناس، من غش فليس منا)[6]، ووجه الاستدلال أن النبي ﷺ أنكر على صاحب الطعام طريقة العرض والإعلان عن الصبرة من خلال إظهار الطعام

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الجيد وإخفاء الرديء وهو شكل من أشكال الغش والخداع[1]، ثم بين ﷺ لصاحب الصبرة كيف يكون الإعلان عن سلعته وفق الضابط الشرعي بقوله: (أفلا جعلته فوق الطعام كي يراه الناس؟).

رابعا ـــ تبيح الشريعة الإسلامية وفق ضوابط محددة كل ما تعلق بحاجة الناس وكانت المصلحة فيها راجحة، تفاديا لوقوع الناس في حرج المشقة المنهي عنها ودليل ذلك قوله تعالى: ﴿ وَمَا جَعَلَ عَلَيْكُمْ فِي ٱلدِّينِ مِنْ حَرَجٍ ﴾[2]، وقوله عز وجل:﴿ يُرِيدُ ٱللَّهُ بِكُمُ ٱلْيُسْرَ وَلَا يُرِيدُ بِكُمُ ٱلْعُسْرَ ﴾ [3]، كما جاء في حديث عائشة رضي الله عنها: (ما خير النبي صلى الله عليه وسلم بين أمرين إلا اختار أيسرهما ما لم يأثم..)[4]، وبالنظر إلى ما تشهده الأسواق التجارية المعاصرة من تنوع هائل في السلع والخدمات فإن مشروعية الإعلان التجاري تساهم في رفع الحيرة والتردد لدى الناس عند اختيارهم لحاجاتهم واتخاذهم للقرار الصائب في الشراء[5]. وكذلك يعتبر الإعلان التجاري في الوقت الحاضر من ضروريات دوران العجلة الاقتصادية والتجارية لما يلحقه من آثار تتعلق بتحسين النوعية ورفع مستوى الإنتاج، ونفي الضرر وإثبات المنفعة وهو من مقاصد الشريعة الإسلامية التي تعززها قواعد نفي الضرر في الفقه الإسلامي كقاعدة " لا ضرر ولا ضرار"[6].

وما يمكن استخلاصه أن الأصل في الإعلان التجاري الإباحة ما لم يروج لسلعة أو خدمة أو منشأة محرمة، أو احتوى تصميمه على ما يحرمه الشارع كعرض العورات أو انطوى على الغش أو الخداع أو التغرير بالمستهلك.

الفرع الخامس: حكم الإعلانات التجارية الكاذبة عبر الانترنت

لا يختلف الحكم الشرعي في تحريم الإعلان التجاري الكاذب سواء كان عبر الانترنت أو أي وسيط إلكتروني أو تقليدي آخر لكونه يقوم على الكذب والغش والخداع، وإنما الاختلاف يحصل في نسبة الضرر الذي يلحقه الإعلان التجاري الكاذب بالضحية عن طريق استعمال الوسائط الإلكترونية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والذي قد يترتب عنه أحكام جنائية إضافية، ففي حالة الإعلان التجاري التقليدي إذا كان كاذبا فإنه من السهولة أن يطالب الضحية باسترجاع ماله، كما يمكنه مقاضاة الجاني وهو ما لا يمكن تحقيقه في حال التعدي عن طريق الانترنت، وقد جاء في البحث محل الدراسة أن من خصائص المجرم المعلوماتي سهولة التخفي ومحو أثر اقتفاءه مما يجعل من الصعوبة معرفة الجاني أو مقاضاته، وهو ما دفع العديد من الجناة إلى استغلال حيل الإعلان التجاري الكاذب عبر الانترنت بغرض بيع كميات قياسية من السلع والخدمات وذلك عن طريق إيهام المستهلك بمواصفات مغرية لا تنطبق حقيقتها على الواقع، أو الإعلان عن عروض وهمية يكون الهدف منها سرقة مال الضحية بما يساوي قيمة السلعة أو الخدمة المزعومة، كما يستخدم الجناة الإعلان كفخ للحصول على المعلومات الشخصية المتعلقة بالضحية كالرقم السري لبطاقة الدفع وما يتعلق بها أثناء إجراء المعاملة ومن ثم الاستيلاء على أمواله، وكلها تصرفات حرمتها الشريعة الإسلامية لاشتمالها على الكذب، والغش، والخداع، والسرقة.

فالضوابط الشرعية للمعاملات المالية تستوجب الصدق في التعامل، والصدق هو الإخبار بالشيء على ما هو عليه وقد قال رسول الله ﷺ: (التاجر الصدوق الأمين يحشر يوم القيامة مع النبيين والصديقين والشهداء)[1]، فاستحق التاجر الصدوق هذه المكانة العالية لما يبذله من مجاهدة لنفسه الطموحة إلى الربح الوافر الذي عادة ما يكون الكذب سبيله الوحيد، وفي هذا السياق قال النبي ﷺ: (التجار يحشرون يوم القيامة فجارا إلا من اتقى الله وبر وصدق)[2]، كما تطرق الفقهاء إلى أهمية الصدق في الإعلان وتحدثوا عن وجوب صدق ما يعرف بالدلال الذي كان ينادي على السلع ويذكر أوصافها، حيث أسقطوا شهادته في حال ما إذا عرف عنه الكذب في إعلاناته كعقوبة تعزيرية له[3].

والكذب في الشريعة الإسلامية من الأخلاق الفاسدة المنهي عنها حيث ورد ذكره في القرآن الكريم ـــ بصيغ مختلفة ـــ من بينها قوله تعالى:﴿ وَيُنذِرَ ٱلَّذِينَ قَالُواْ ٱتَّخَذَ ٱللَّهُ وَلَدًا ۝ مَّا لَهُم بِهِۦ مِنْ عِلْمٍ وَلَا لِأَبَآئِهِمْ كَبُرَتْ كَلِمَةً تَخْرُجُ مِنْ أَفْوَٰهِهِمْ إِن يَقُولُونَ إِلَّا كَذِبًا ﴾ [4]، وقوله عز وجل:﴿ وَلَا تَقُولُواْ لِمَا تَصِفُ أَلْسِنَتُكُمُ

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

ٱلْكَذِبَ هَٰذَا حَلَٰلٌ وَهَٰذَا حَرَامٌ لِّتَفْتَرُواْ عَلَى ٱللَّهِ ٱلْكَذِبَ ۚ إِنَّ ٱلَّذِينَ يَفْتَرُونَ عَلَى ٱللَّهِ ٱلْكَذِبَ لَا يُفْلِحُونَ ﴾ [1]، ومن السنة قوله ﷺ : (عليكم بالصدق، فإنه يهدي إلى البر وإن البر يهدي إلى الجنة، وإن الرجل ليصدق حتى يكتب عند الله صديقا، وإياكم والكذب، فإن الكذب يهدي إلى الفجور، وإن الفجور يهدي إلى النار، وإن الرجل ليكذب حتى يكتب عند الله كذابا)[2]، وهي أدلة تفيد تحريم الكذب ولا يختلف حكمه باختلاف المكان والزمان أو اجتهاد الحاكم، حيث يعتبر جريمة يحد عليه في القذف، ويعزر عليه في بقية صوره، ولذلك يحرم الكذب في الإعلان عن السلع والخدمات، وهو ما ينطبق أيضا على الإعلان التجاري المبني على الغش والخداع باعتباره من التصرفات المحرمة شرعا ودليل ذلك من الكتاب والسنة والإجماع كما يلي:

قال تعالى:﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٍ مِّنكُمْ ﴾[3]، فوجوب الرضا هو من أركان المعاملات المالية التي تبيح انتقال التملك بين الناس ولا شك أن الغش والخداع في التعامل يتنافى ومبدأ الرضا مما يؤول إلى أكل المال بالباطل وهو محرم بالنص الثابت.

ومن السنة النبوية الشريفة قوله ﷺ لصاحب صبرة الطعام الذي أظهر الجاف وأخفى المبتل: (أفلا جعلته فوق الطعام كي يراه الناس، من غش فليس منا)[4]، وهو حكم يفيد تحريم إظهار المبيع على صفة لا تنطبق عليه الحقيقة، والإعلان التجاري الكاذب ما هو إلا إظهار المبيع على صفة ليست هي عليها في الحقيقة وهو لا يجوز شرعا.

وجاء أيضا في حديث التصرية[5] قوله ﷺ: (لا تصرّوا الإبل والغنم، فمن ابتاعها بعد فإنه بخير النظرَيْنِ بعدَ أن يحتلبها: إن شاء أمسك، وإن شاء ردّها وصاع تمر)[6]، فالنبي ﷺ نهى عن التصرية لما فيها من غش وخداع المشتري من خلال إظهار الناقة أو الشاة على أنها حلوب مع أنها ليست

---

(1) الإحالات في النسخة المطبوعة

(2) الإحالات في النسخة المطبوعة.

...../...

كذلك[1]، وهو ما ينطبق على الإعلانات الكاذبة لما تحتويه من غش وخداع المتلقي كالتصرية التي تظهر المبيع بمظهر حسن مع أنها ليست كذلك وهو منهي عنه.

وقد أجمع العلماء على حرمة الغش[2]، ولاشك أن الإعلانات التجارية الكاذبة تبنى على الكذب والغش والخداع فتكون محرمة شرعا.

وبناء على ما تقدم فإنه يحق للمتضرر في معاملة مالية نتيجة الإعلانات الكاذبة عبر الانترنت أن يفسخ العقد ويطالب بالتعويض، كما يخضع المعلن إلى عقوبات تعزيرية وفق ما يقدره الإمام وهو حكم دنيوي ناهيك عن الحكم الأخروي، أما إذا اشتملت المعاملة على سرقة المال فإن الجاني قد يتعرض إلى حد السرقة إن تحققت شروط ذلك كما سبق ذكره، وإضافة إلى الضرر المادي الذي تلحقه الإعلانات التجارية الكاذبة بالمستهلكين فقد ينعكس ذلك على نفسيتهم نحو التثبيط والإحباط من التعامل عن طريق التجارة الإلكترونية رغم كونها من ضرورات العصر، وعلى أساس ذلك فإن الإمام في تقديره للعقوبات التعزيرية في مثل هذه الحالة يأخذ بالاعتبار مدى الضرر الذي لحق المصلحة العامة والخاصة بسبب هذا النوع من التصرفات المحرمة.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الثاني:
جرائم التعدي على النفس والعرض

المبحث الأول: القذف والتشهير الإلكتروني.

المبحث الثاني: جرائم التعدي على البريد الإلكتروني.

المبحث الثالث: جريمة صناعة المواقع الإباحية وترويجها عبر الانترنت

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: القذف والتشهير الإلكتروني

يعد القذف والتشهير من الجرائم البشعة التي تؤثر على شخص الإنسان وكرامته، وقد زادت حدتهما بعد ظهور شبكة الانترنت حيث اتخذها الكثير من المغرضين كأداة للنيل من شرف الغير سواء كان حاكما أو محكوما، فردا أو جماعة، دون الخوف من الملاحقة القضائية نتيجة ما تتيحه هذه التكنولوجيا من خصائص التنصل من الجريمة. ولقد أصبحت صور القذف والتشهير الإلكتروني لا تعد ولا تحصى؛ حيث تنشر على شكل نصوص يتعرض فيها الضحية إلى شتى أنواع القذف والكلام الفاحش والتشهير بشخصه أو بأسرته، كما تنشر على شكل صور مفبركة لإهانة الضحية والسخرية منه أو من خلقته، وأحيان تنشر صور خصوصية عن الضحايا بغرض فضحهم والإطاحة من شخصيتهم، إضافة إلى إنتاج ونشر لقطات سمعية بصرية لا تعد ولا تحصى يتفنن فيها مخرجوها بشتى الخدع التقنية والدبلجة الصوتية ليلحقوا أقصى درجات الأذى بالضحايا الذين عادة ما يمثلون رموزا سياسية أو دينية وغيرها.

أما أغراض هذه التصرفات فتتفاوت؛ ابتداء من السخرية والاستهزاء ووصولا إلى درجة إثارة الفتنة في المجتمع وزعزعة أمنه واستقراره خاصة وأن وسائل تكنولوجيا الإعلام والاتصال أثبتت مدى تأثيرها السلبي أو الإيجابي على عقول الأفراد والمجتمعات المعاصرة.

وإدراكا من الشارع الكريم لمدى خطورة هذه الجرائم جعل حفظ العرض من الضرورات الخمس التي تقوم عليها مقاصد الشريعة الإسلامية، لأن حماية حرمات المسلمين لا تقل أهمية عن الطعام والشراب بل هي من أعظم الضرورات التي تتوقف عليها سعادة الأسرة والمجتمع، ولذلك فإن حياة المسلم مقدسة لا يجوز التعدي عليها بأي حال كان وهو ما أقرته الشريعة الإسلامية انطلاقا من قول الرسول ﷺ في خطبة الوداع: (فإن دماءكم وأموالكم وأعراضكم عليكم حرام، كحرمة يومكم هذا، في شهركم هذا، في بلدكم هذا)[1].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الأول: مفهوم القذف الإلكتروني وحكمه

الفرع الأول: تعريف القذف لغة واصطلاحا

أولا ــ تعريف القذف لغة:

القذف في اللغة هو الرمي مطلقًا، ومنه الرمي بالحجارة ونحوها ثم استعمل في الرمي بالمكاره لعلاقة المشابهة بين الحجارة في تأثير الرمي بكل منهما وما ينتج عن ذلك من أذى، وأصل القذف الرميُ من بُعد، ويطلق أيضا على السب والشتم[1].

ثانيا ــ التعريف الاصطلاحي للقذف:

عرّف الفقهاء القذف بتعريفات عدة أهمها:

ــ القذف عند الحنفية "هو رمي الرجل رجلاً محصنًا أو امرأة محصنة بصريح الزنا"[2]، بمعنى أن القذف قد يكون بلفظ صريح لا يحتمل غير الاتهام بالزنا أو نفي النسب[3].

ــ أما القذف عند المالكية فهو قسمان: قذف أعم يشمل ما يوجب الحد وما لا يوجب بأن كان صادقا، وقذف أخص وهو الموجب للحد؛ ويعرّف القذف الأعم: " نسبة آدمي غيره لزنى أو قطع نسب مسلم"[4]، والقذف الأخص: " هو نسبة آدمي مكلف غيره حرا عفيفا بالغا أو صغيرة تطيق الوطء لزنى أو قطع نسب مسلم"[5]، ويقصد بالمكلف أن يكون القاذف عاقلا بالغا غير مكره، ولفظ "غيره" هو المقذوف ويشترط فيه الحرية والإسلام والعفاف والبلوغ ويضاف إلى ذلك الصغيرة التي تطيق الوطء[6].

ــ وقال الشافعية في القذف:" هو الرمي بالزنى في معرض التعيير"[7].

ــ وأما الحنابلة فعرفوا القذف " بأنه الرمي بالزنا"[8].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ وعرفه الظاهرية أيضا " بأنه الرمي بالزنا"[1].

وما يستخلص من خلال هذه التعريفات أن المفهوم الاصطلاحي للقذف هو رمي المحصن بالزنى أو بنفي النسب سواء كان القاذف محصنا أو غير محصن[2]، كما يوجب الحد في القذف الصريح والكناية على السواء.[3]

ثالثا ـــ تعريف القذف الإلكتروني:

لا يخرج تعريف القذف الإلكتروني عن القذف الاصطلاحي إلا في نوع الوسيلة المشهر بها وهي الانترنت أو الوسائل الإلكترونية المشابهة، ولذلك يمكن تعريف القذف الإلكتروني بناء على التعريفات الاصطلاحية بأنه: نسبة آدمي غيره لزنى أو قطع نسب مسلم عن طريق وسائل الإعلام والاتصال الحديثة.

ولذلك فإن القذف عبر الانترنت أو الوسائل المشابهة يأخذ نفس حكم التلفظ به؛ بجامع أنهما يؤذيان صاحبهما ويوقعانه في الضرر، والذي ينظر في واقع الانترنت خاصة منها مواقع التواصل الاجتماعي ومواقع الحوار والنقاش يجد جرأة الكثير من المشتركين على السب والقذف الذي يأنف منه المسلم ويخشى عقوبته، وهو ما يدعو إلى بيان حكمه الشرعي وذلك من القرآن والسنة والإجماع.

الفرع الثاني: حكم القذف الإلكتروني

يعد القذف في الشريعة الإسلامية من الكبائر التي ثبت تحريمها بالكتاب والسنة والإجماع:

أولا ـــ حكم القذف في القرآن:

قال تعالى:﴿ وَٱلَّذِينَ يَرْمُونَ ٱلْمُحْصَنَٰتِ ثُمَّ لَمْ يَأْتُوا۟ بِأَرْبَعَةِ شُهَدَآءَ فَٱجْلِدُوهُمْ ثَمَٰنِينَ جَلْدَةً وَلَا تَقْبَلُوا۟ لَهُمْ شَهَٰدَةً أَبَدًا ۚ وَأُو۟لَٰٓئِكَ هُمُ ٱلْفَٰسِقُونَ ﴾ [4]،ووجه الدلالة من الآية في قوله تعالى:﴿ وَٱلَّذِينَ يَرْمُونَ ٱلْمُحْصَنَٰتِ﴾ تدل بمنطوقها على عموم القذف بغض النظر عن الطريقة فيكون القذف عبر الانترنت مندرجا ضمنه،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما أن الرمي بالزنا لا بد أن يكون ثابتا بشهادة أربعة من الشهداء لتبرئة ذمة القاذف وإن لم يكن ذلك فإنه يجلد ثمانين جلدة وهي لا تقبل استبدالا ولا إنقاصا وليس لولي الأمر حق العفو عنها، كما تهدر كرامته الإنسانية فلا تقبل شهادته باعتباره فاسق خارج عن طاعة الله عز وجل لأنه دنس لسانه بقول أفحش الباطل وأخبثه[1]، وهذا نص صريح في وجوب معاقبة القاذف بما نصت عليه الآية.

وقال تعالى:﴿ إِنَّ ٱلَّذِينَ يَرْمُونَ ٱلْمُحْصَنَٰتِ ٱلْغَٰفِلَٰتِ ٱلْمُؤْمِنَٰتِ لُعِنُواْ فِى ٱلدُّنْيَا وَٱلْءَاخِرَةِ وَلَهُمْ عَذَابٌ عَظِيمٌ ﴿٢٣﴾ يَوْمَ تَشْهَدُ عَلَيْهِمْ أَلْسِنَتُهُمْ وَأَيْدِيهِمْ وَأَرْجُلُهُم بِمَا كَانُواْ يَعْمَلُونَ ﴿٢٤﴾ يَوْمَئِذٍ يُوَفِّيهِمُ ٱللَّهُ دِينَهُمُ ٱلْحَقَّ وَيَعْلَمُونَ أَنَّ ٱللَّهَ هُوَ ٱلْحَقُّ ٱلْمُبِينُ ﴾ [2]، ووجه الاستدلال من النص أن القذف هو من الكبائر ولذلك فإن الذي يرمي المؤمنة الحرة أو المؤمن الحر بالزنا ملعون في الدنيا، وهو مطرود من رحمة الله في الآخرة وله عذاب شديد[3].

ثانيا ــ حكم القذف في السنة:

قال النبي ﷺ: (اجتنبوا السبع الموبقات، قالوا وما هن يا رسول الله؟ قال: الشرك بالله، والسحر، وقتل النفس التي حرم الله إلا بالحق، وأكل الربا، وأكل مال اليتيم، والتولي يوم الزحف، وقذف المحصنات الغافلات)[4].

ووجه الاستدلال، أن رسول الله ﷺ صنف قذف المحصنات الغافلات ضمن الموبقات، فجعله معصية ضمن الشرك بالله وهو من الكبائر التي تستوجب العذاب ولو كان عبر الانترنت لأن المقذوف عادة يكون إنسان غافل ولربما لم يعلم أن أحدا قذفه.

ثالثا ــ حكم القذف في الإجماع:

قال الحافظ ابن حجر: "وقد انعقد الإجماع على أن حكم قذف المحصن من الرجال حكم قذف المحصنة من النساء"[5] ، وقال ابن تيمية: " ومن الحدود التي جاء بها الكتاب والسنة وأجمع عليها المسلمون حد القذف، فإذا قذف الرجل محصنا بالزنا أو اللواط وجب عليه الحد ثمانون جلدة،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والمحصن هنا هو الحر العفيف"[1]، وأجمع العلماء على تحريم القذف كما أجمعوا على وجوب الحدِّ على من قذف المحصن إذا كان مكلفا وفيه الحد وفق شروط معينة[2]، وما دام القذف عبر الانترنت له نفس النتائج المترتبة على القذف الاصطلاحي فيتناوله الحكم بالإجماع حيث لا يعرف له مخالفا.

كما أن نسبة الضرر الذي يحدثه القاذف عبر الانترنت تكون جسيمة لأن القذف يصل إلى أكبر عدد ممكن من المجتمع المعلوماتي المتواجد في كافة بقاع العالم، فيكون من الواجب الحكم بالحد وهو الجلد ثمانين جلدة، وبطلان الشهادة، والحكم بتفسيق القاذف إلى أن يتوب[3].

المطلب الثاني: مفهوم التشهير الإلكتروني وحكمه

الفرع الأول: تعريف التشهير لغة واصطلاحا

أولا ــ تعريف التشهير لغة:

التشهير في اللغة مأخوذ من شهره، بمعنى: أعلنه وأذاعه، وشهّر به: أذاع عنه السوء، والشهرة الفضيحة[4].

ثانيا ــ تعريف التشهير اصطلاحا:

لا يخرج تعريف التشهير عند الفقهاء عن معناه في اللغة، إذ هو إظهار الشخص بفعل، أو عيب يفضحه ويشهره بين الناس[5].

ثالثا ــ تعريف التشهير الإلكتروني

إن استطلاعي على مواقع الانترنت خاصة منها مواقع الحوار والنقاش والتواصل الاجتماعي جعلني أجزم إلى أن مسألة التشهير بالأشخاص هي أكثر ما يحكى فيها، بل هناك العديد من المواقع صممت خصيصا للتشهير بالأشخاص والتنكيل بهم، وقد عرفت هذه المواقع رواجا كبيرا لدى فئات عديدة من الناس حتى جعلوا منها ثقافة يتسلون فيها بالاطلاع على عيوب الناس و يتفننون في

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

فضحهم والتشهير بهم، وما يلاحظ على أساليب التشهير في الانترنت أنها لا تخرج في مجملها عن الآتي:

أولا ــ الألفاظ المتعاملة:

ــ ألفاظ لها علاقة بالقذف تبين أن الشخص كان من الزناة، ومثال ذلك: كان زانيا، أو يفعل فعل قوم لوط، أو هو ابن زنا، أو ابن زانية..

ــ ألفاظ تمس الأخلاق ككون الشخص من رواد السهرات الماجنة، أو زير نساء، كثير السفر إلى دول الخنا، يرتاد الملاهي والخمارات ...

ــ ألفاظ تمس أمانة الشخص؛ ككونه غير نزيه، لا يتقي الله في كذا، غير أمين، مصلحي، مرتشي، ... الخ.

ــ ألفاظ تمس عقيدة الشخص؛ ككونه ليبرالي، علماني، وهابي، صوفي، شيعي، أصولي متشدد..

ثانيا ــ الصور ولقطات الفيديو:

لا يخلو الأمر من نشر الصور ولقطات الفيديو من أن تكون حقيقية أو كذبا مركبا، والحقيقية تكون في أمرين:

1 ــ نشر صورة أو فيديو واقعي عن الضحية؛ كتقبيل امرأة تحل أو لا تحل له، أو يكون مختليا بامرأة تحل له أو لا تحل.

2 ــ نشر صورة أو فيديو لشخص مرموق اجتماعيا في وضع غير لائق يستوجب الخصوصية.

أما الصور ولقطات الفيديو الكاذبة فهي ثلاثة أنواع:

1 ــ تركيب صورة أو فيديو للشخص المشهر به في أوضاع مخلة بالآداب العامة والأخلاق.

2 ــ تركيب صورة أو فيديو للشخص المشهر به ليسخر منه العامة، كأن يركب وجهه على حيوان، أو مغنٍ، أو ممثل، أو لاعب كرة بغرض التنكيل والاستهزاء به.

3 ــ تركيب صورة أو فيديو للشخص المشهر به يعاقر الخمر، أو يلعب القمار ونحوه.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وبناء على ذلك فإن التشهير الإلكتروني لا يخرج تعريفه عن معناه في اللغة والاصطلاح الفقهي حيث يمكن تعريفه بأنه: إظهار الشخص بفعل، أو عيب يفضحه ويشهره بين الناس عن طريق الانترنت أو وسائل تكنولوجيا الإعلام والاتصال.

الفرع الثالث: حكم التشهير بالغير

التشهير في الفقه الإسلامي محرم بالكتاب، والسنة، والإجماع وبيانه كما يلي:

أولا: من القرآن الكريم قوله تعالى:﴿ إِنَّ ٱلَّذِينَ يُحِبُّونَ أَن تَشِيعَ ٱلْفَٰحِشَةُ فِى ٱلَّذِينَ ءَامَنُواْ لَهُمْ عَذَابٌ أَلِيمٌ فِى ٱلدُّنْيَا وَٱلْءَاخِرَةِ ۚ وَٱللَّهُ يَعْلَمُ وَأَنتُمْ لَا تَعْلَمُونَ ﴾ [1]، قال ابن كثير: " إن في هذا تأديب لمن سمع شيئا من الكلام السيئ فقام بذهنه منه شيء، وتكلم به، فلا يكثر منه ويشيعه ويذيعه".[2]

وقال تعالى:﴿ وَٱلَّذِينَ يُؤْذُونَ ٱلْمُؤْمِنِينَ وَٱلْمُؤْمِنَٰتِ بِغَيْرِ مَا ٱكْتَسَبُواْ فَقَدِ ٱحْتَمَلُواْ بُهْتَٰنًا وَإِثْمًا مُّبِينًا ﴾[3]، ووجه الاستدلال من الآية أن الله تعالى حرم الإيذاء بأشكاله على عباده المؤمنين والمؤمنات، والتشهير من البهتان فيؤذي المؤمنين والمؤمنات بالذم والتجريح والنيل منهم، ولقد قال أبو بكر الجزائري في أيسر التفاسير: إن الذين يؤذون رسول الله ﷺ بانتقاص أو تعرض له أو لآل بيته أو أمته أو سنته أو دينه هؤلاء "لعنهم الله في الدنيا والآخرة" أي طردهم من رحمته، "وأعد لهم" أي هيأ له عذابا مهينا لهم يذوقونه بعد موتهم ويوم بعثهم يوم القيامة[4].

ثانيا: دليل تحريم التشهير من السنة النبوية؛ أن ابن عمر رضي الله عنهما قال: (صعد رسول اللهﷺ المنبر فنادى بصوت رفيع، فقال: يا معشر من قد أسلم بلسانه و لم يفض الإيمان إلى قلبه، لا تؤذوا المسلمين، ولا تعيروهم، ولا تتبعوا عوراتهم، فإنه من تتبع عورة أخيه المسلم تتبع الله عورته، ومن تتبع الله عورته يفضحه، ولو في جوف رحله)[5]، وهو حديث ينهى عن التشهير بالمسلمين وتتبع عوراتهم، ويتوعد فيه النبي ﷺ الذي يتتبع عورات الناس بأن الله سيتتبع عورته وسيفضحـــه ولو كان

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

متخفيا في وسط بيته[1]، وهذا دليل على أن التشهير من أشد المنكرات وأعظم المحرمات.

وجاء في حديث آخر، عن جندب بن عبد الله البجلي رضي الله عنه، أن رسول الله ﷺ قال: (من سمّع سمّع الله به، ومن يُرائى يُرائي الله به)[2]، فمن سمّع (أي شهّر) بعيوب الناس وأذاعها، فإن الله سيظهر عيوبه بأن يشهره ويفضحه وهي عقوبة تفيد تحريم التشهير بالناس[3].

ثالثا: تحريم التشهير بالإجماع؛ لقد أجمع أهل العلم منذ القدم إلى يومنا هذا على وجوب صون أعراض المسلمين، وحرمتها[4]، وحتى وإن كان المشهر به يتصف بما يقال عنه ولكنه لا يجاهر به ولا يقع به ضرر على غيره فيحرم التشهير به لأنه من الغيبة التي نهى الله سبحانه وتعالى عنها في قوله: ﴿وَلَا يَغْتَب بَّعْضُكُم بَعْضًا﴾[5]، كما أنه من المقرر شرعا أن الستر على المسلم واجب لمن ليس معروفا بالأذى والفساد، وقد قال النبي ﷺ : (من ستر مسلما ستره الله عز وجل يوم القيامة)[6].

وما نخلص إليه أن التشهير الإلكتروني محرم شرعا وعقوبته واجبة لما فيها من درء المفاسد، حيث يتلقى الجاني إضافة إلى العقاب الرباني عقوبة التعزير وذلك حسب ما يقدره الإمام باعتبار ما نتج عن الجريمة من أذى، كما تخضع جناية التشهير إلى عقوبة حد القذف المنصوص عليه شرعا إذا توفرت فيها شروطه[7].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني:
جرائم التعدي على البريد الإلكتروني

يعد البريد الإلكتروني من أهم ما وفرته التكنولوجيا الحديثة حيث يلعب دورا فعالا في تواصل الأفراد والمجتمعات على المستوى العالمي، كما يعد من الضرورات المعاصرة التي لا يستغنى عنها معظم الناس بالنظر إلى ما يوفره من تيسير الخدمات والمصالح في شتى الميادين الاجتماعية منها والتجارية والتربوية وغيرها، كما تجاوزت أهميته المصالح الشخصية إلى المسائل العامة في ظل التطور الذي يشهده العالم وقيام ما يعرف بالحكومات الإلكترونية التي تقوم أساسا على مسألة التواصل مع البريد الإلكتروني.

وحقيقة البريد الإلكتروني هو تجسيد إلكتروني مجازي لنظام البريد التقليدي المعروف، ورسائله عبارة عن وثائق إلكترونية مشفرة رقميا (ASCII) كالتي تحرر بواسطة برامج معالجة الكلمات وليست حبرا على ورق كما كانت عليه سلفا، ويتم إرسالها على شكل نبضات كهربائية عبر الشبكة العالمية وليس ضمن مظاريف مختومة ومدموغة بالطوابع البريدية، كما تستقر هذه الرسائل في مساحة محددة من القرص الثابت لحاسوب الطرف المستقبل، وليس في صندوق معدني أو خشبي في مكاتب البريد المحلية[1]. كما لا يتطلب البريد الإلكتروني أكثر من امتلاك عنوان إلكتروني يعرف بـــ E-mail الذي يقوم بدور العنوان البريدي التقليدي، ويتألف العنوان الإلكتروني عموما من عدة مقاطع لكل منها دلالة اصطلاحية معروفة.

المطلب الأول: مفهوم البريد الإلكتروني لغة واصطلاحا

الفرع الأول: تعريف البريد الإلكتروني في اللغة

يتركب لفظ البريد الإلكتروني من مفردتين: " البريد " و "الإلكتروني " وتعريفهما كما يلي:

أولا ـــ البريد: يقصد بالبريد لغة؛ فرسخان، وقيل: ما بين كل منزلين بريد، والبريدُ: الرسل على دوابّ البريد والجمع بُرُد وبَرَدَ بريدًا: أرسله[2].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وجاء في الصحاح: البريد المُرتَّبُ، يقال: حمل فلان على البريد، والبريد أيضا: اثنا عشر ميلا[1].

كما اختلف اللغويون في أصل الكلمة، فقيل إنها عربية ومعناه "الرسول"، وذهب آخرون إلى أن اللفظ فارسي الأصل ومعرب، وأصله بالفارسية "بريدة دم" ومعناه "مقطوع الذنب"[2].

ثانيا ــ الإلكتروني: لفظ الإلكتروني لغة نسبة إلى "الإلكترون" وهي كلمة انجليزية الأصل Electronic، وعُرف الإلكترون بأنه: دقيقة ذات شحنة كهربائية سالبة شحنتها هي الجزء الذي لا يتجزأ من الكهرباء[3].

الفرع الثاني: تعريف مصطلح البريد الإلكتروني

نظرا لكون مصطلح البريد الإلكتروني حديث نسبيا فلم أعثر حسب اطلاعي على تعريف له في الاصطلاح الفقهي، أما من ناحية الاصطلاح الوضعي فقد عرف العديد من التعريفات أهمها:

البريد الإلكتروني هو طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات[4].

و يعرّف بأنه: تلك المستندات التي يتم إرسالها أو استلامها بواسطة نظام اتصالات بريدي إلكتروني، وتتضمن ملحوظات مختصرة ذات طابع شكلي حقيقي، ويمكنه اصطحاب مرفقات به وأية مستندات أخرى يتم إرسالها رفقة الرسالة ذاتها[5].

ويعرّف أيضا بأنه: وثيقة معلوماتية يحررها أو يرسلها أو يطلع عليها المستخدم عن طريق الاتصال بشبكة معلومات[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

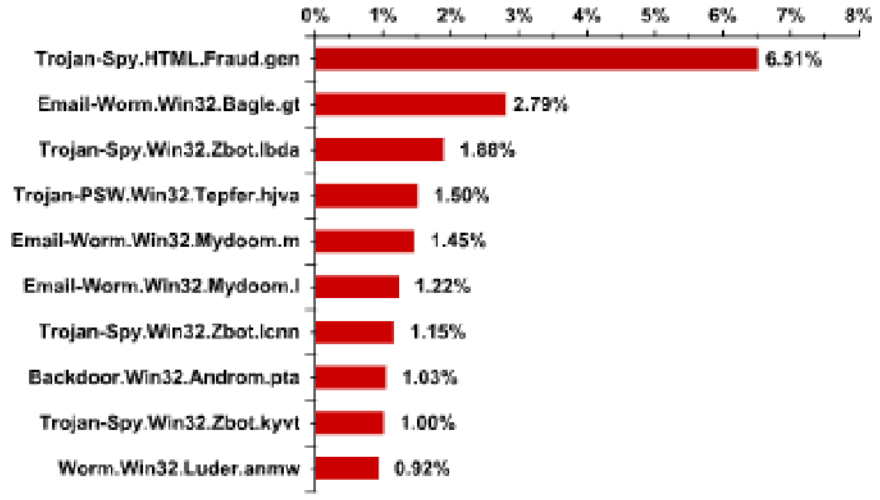
...../...

المطلب الثاني: صور التعدي على البريد الإلكتروني

تعتبر الرسائل والبيانات التي يتضمنها البريد الإلكتروني ترجمة لأفكار شخصية أو آراء خاصة لا يجوز لغير مصدرها ومن توجه إليه الاطلاع عليها وإلا كان ذلك انتهاك لحرمة المراسلات وهو ما يعني انتهاك الحياة الخاصة، فحرية المراسلات تعد من العناصر الضرورية في الحياة الخاصة والحريات الشخصية وما الرسالة إلا مستودع للسر ولخصوصيات الإنسان، لذلك لا يجوز انتهاك سرية هذه المراسلات ولا يجوز أن يسترق إلى هذه المحادثات أو يفشى سرها[1].

وبالرغم من ذلك فإن الدراسات المتخصصة أثبتت أن البريد الإلكتروني هو أحد أكبر مصادر التجسس و العبور إلى داخل الأنظمة المعلوماتية كما سبق بيانه في البحث، حيث تعد الرسائل الإلكترونية أكثر مصادر الخطر التي يتم من خلالها تمرير برامج الفيروسات والديدان وبرامج التجسس على النظام الحاسوبي الخاص بالمستخدمين المستهدفين وإعادة توجيه المعلومات خفية للطامعين، وتبرز حجم المشكلة الحقيقية عندما تكون المعلومات ذات قيمة إستراتيجية أو اقتصادية أو عسكرية أو دبلوماسية أو حتى ذات أهمية علمية مما يشكل ضررا جسيما على أصحابها[2].

والرسم البياني التالي يبين أهم البرامج الخبيثة المرفقة التي رصدتها دراسة أجريت حول رسائل البريد الإلكتروني الحاملة للفيروسات خلال سنة 2013م[3]:



الشكل رقم (32): يوضح أهم المرفقات الخبيثة ونسبها في رسائل البريد الإلكتروني

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

ومن أبرز صور التعدي على البريد الإلكتروني ما يلي:

الفرع الأول: اختراق البريد الإلكتروني

يُعرف الاختراق بالقرصنة Hacking [1]، ويعرّفه القانون النموذجي العربي الموحد بأنه: الدخول غير المصرّح به، أو غير المشروع لنظام المعالجة الآلية للبيانات، وذلك عن طريق انتهاك الإجراءات الأمنية[2]، وهو تصرف يتم بواسطته اختراق البريد الإلكتروني وانتهاك سريته، مما يتيح للجاني تغيير محتوياته أو سرقتها، أو التجسس على الضحية، أو تدمير الأنظمة المعلوماتية.

ويعتمد الجاني في عملية اختراق البريد الإلكتروني على بعض البرامج والوسائل، من أهمها: برامج أحصنة طروادة Trojan Horses التي سبق التكلم عنها في البحث، أما ضررها فيكمن في إتاحة التجسس على الضحية والتعرف على كلمات العبور وتدمير الملفات[3]، كما يتم الاختراق أيضا عن طريق الملفات المعروفة بـــ " الكوكي Cookie " وهي ملفات صغيرة تمثل المواقع التي يزورها المستخدم وتثبت تلقائيا على قرصه الصلب لأهداف تجارية، لكنه كثيرا ما يساء استخدامها بغرض الحصول على معلومات المستخدم ومنها مفاتيح البريد الإلكتروني[4].

الفرع الثاني: التعدي على البريد الإلكتروني بالرسائل الاقتحامية SPAM

تُعرف الرسائل الاقتحامية بمسميات عدة مثل: البريد المزعج، وبريد القمامة، والبريد التطفلي، والرسائل غير المرغوبة وغيرها، ويقصد بها: إساءة استخدام نظام الرسائل الإلكترونية ـــ Electronic Messaging System ـــ بإرسال كم هائل من الرسائل العشوائية غير المطلوبة، أو غير المتوقعة أو غير المرغوبة من قبل المستقبلين لها.[1]

وتعد الرسائل الاقتحامية من بين أنجح السبل المستخدمة في الاحتيال والقرصنة ونشر البرمجيات الضارة، حيث يقول في شأنها خبراء أمن المعلومات؛ هي عبارة عن مجموعة من رسائل ترسل بكميات هائلة من قبل مجموعة أشخاص يعرفون باسم "Spammers"، وهم المتطفلون الذين يكسبون أموالهم

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../.....

من تلك النسب الصغيرة من المستخدمين الذين يستجيبون لرسائلهم، كما يؤكد نفس الخبراء على أن البريد المزعج لا يزال يشكل خطراً حقيقياً على مستخدمي البريد الإلكتروني والشبكة، خصوصا في ظل تطور تقنيات المتطفلين وتصديهم لبرامج الحماية، وهذا ما يبقي الحرب قائمة[1].

ويستخدم مرسلو الرسائل الإلكترونية المزعجة العديد من الأساليب والحيل التي يكون هدفها في الغالب توليد الأرباح والنصب والاحتيال على حساب الغير حيث تحمل هذه الرسائل في غالبيتها روابط وإعلانات دعائية وبمجرد نقر المستخدم عليها يتحصل المرسل أو المتطفل على عمولة معينة، وما يجب التنويه له أن أكبر الأرباح تأتي من الرسائل الاقتحامية التي تحتوي على برامج خبيثة[2].

الفرع الثالث: التعدي على البريد الإلكتروني عن طريق الرسائل الاحتيالية

تعرف الرسائل الاحتيالية في البريد الإلكتروني برسائل الاصطياد الإلكتروني Phishing أو الرسائل المخادعة، لأن الجناة يستخدمونها كطعم لاصطياد كلمات المرور السرية وغيرها من البيانات الشخصية الحساسة من مستخدمي الشبكة العالمية[3]، كانتحالهم لشخصية ما، كمصرف أو هيئة معينة يتم فيها إيهام الضحية بجدية الطلب وأهميته على مصلحته الخاصة وذلك بغرض الحصول على بياناته المالية أو ملفاته الخاصة والتي تستغل حسب أغراض الجريمة.

ومن الأضرار التي تسببها الرسائل الاحتيالية، تعطيل الخدمة التي يقوم بها البريد عن طريق دس برامج خبيثة يتم تفعيلها بمجرد قراءة الرسالة مما يترتب عليه خسائر مادية تلحق بالمؤسسات التجارية خاصة المنافسة منها[1].

المطلب الثالث: أهداف التعدي على البريد الإلكتروني

تختلف أهداف اختراق البريد الإلكتروني حسب دوافع المجرمين التي يسعون من خلالها، ولعل من أبرزها[2]:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

1 ــ سرقة المال، وهو أحد الدوافع الأساسية التي يسعى من خلالها الجناة إلى اختراق البريد الإلكتروني مستعينين في ذلك بجميع الطرق غير المشروعة لاختراق أجهزة المستخدمين وبالتالي سرقة المعلومات الهامة، مما يلحق أضرارا جسيمة بالضحية كاستخدام حسابه البنكي لطلب قروض مالية، أو عمليات نقل الأموال أو التسوق عبر الانترنت على حسابه الخاص وغيرها من أوجه التعدي المختلفة في هذا المجال.

2 ــ التجسس، وهو من الدوافع البارزة لعمليات الاختراق الإلكتروني التي تطال الأفراد أوالمؤسسات، أو المنظمات، أو الدول، وتتفاوت خطورته وأضراره بحسب سعي الجناة من وراءه، فقد يكون الهدف منه تتبع عورات الضحايا وابتزازهم بالتشهير أو القذف مقابل المال أو دونه، كما قد يكون الهدف منه تنافسيا وذلك بالاطلاع على الرسائل الإلكترونية للمنافسين بغرض معرفة الأنشطة التي يقومون بها من صفقات أو أعمال مصرفية أو مشاريع مستقبلية، أو اكتشافات علمية والتي من خلالها تمكن الجهة المتجسسة من السبق في الحصول على الصفقات أو المشاريع أو السبق في إعلان الاكتشافات العلمية لكسب الحقوق المترتبة عليها.

3 ــ الفضول والعبث، وقد يقع أيضا التعدي بدواعي الفضول والعبث للتباهي أو التحدي بإثبات القدرة على اختراق البريد الالكتروني، حيث يقوم الجاني بترك رسالة لصاحب البريد الإلكتروني المخترق يشعره فيها بأن بريده الإلكتروني تم اختراقه وكأنه يثبت له بأن وسائل الحماية لا تجدي نفعا أمام قدراته الفنية، وقد يتلقف الجاني مجموعة من المعلومات الخاصة بصاحب البريد الإلكتروني ومفاجأته بها أو نشرها في أوساط المعارف والأصدقاء بقصد العبث والمزاح رغم عدم مشروعية هذا التصرف.

المطلب الرابع: حكم التعدي على البريد الإلكتروني

من حق صاحب البريد الإلكتروني الانتفاع به كونه المالك الشرعي له، ولذلك يخضع كل متعد على هذا الحق إلى العقوبة مع الضمان، وهو ما أجمع عليه جمهور الفقهاء من المالكية والشافعية والحنابلة باعتبار أن المنافع أموال متقومة في ذاتها كالأعيان سواء بسواء إذا كان الانتفاع بها مشروعا،

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وتأسيسا على ذلك ترِدُ عليها العقود الناقلة للملكية وتضمن بالغصب، بمعنى أنه تتقرر مسؤولية غاصب مصادرها أو محالّها بالتعويض[1].

وقد نهى الله عز وجل عن الغصب فقال في كتابه الحكيم:﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَأۡكُلُوٓاْ أَمۡوَٰلَكُم بَيۡنَكُم بِٱلۡبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٖ مِّنكُمۡۚ ﴾ [2]، وقال جل وعلا:﴿ وَلَا تَأۡكُلُوٓاْ أَمۡوَٰلَكُم بَيۡنَكُم بِٱلۡبَٰطِلِ ﴾[3]، ووجه الاستدلال من الآيتين تحريم الاستيلاء على مال الغير غصبا بغير حق، ومن السنة النبوية الشريفة أن النبي ﷺ قال: (كل المسلم على المسلم حرام، دمه وماله وعرضه)[4]، كما أجمع المسلمون على تحريم الغصب جملة[5].

ولما كان الغصب محرما شرعا بأي حيلة كانت فإن اختراق البريد الإلكتروني هو تصرف محرم قياسا على ذلك، ويوجب التعزير وفق ما يقدره الإمام مع الضمان، هذا وقد تم التفصيل في مسألة سرقة المال المعلوماتي وإتلافه سابقا.

كما أن التجسس على محتويات البريد الإلكتروني هو خرق لخصوصية الآخرين وهتك حرماتهم، وحكمه التحريم في الكتاب والسنة؛ فقد قال الله سبحانه وتعالى:﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرٗا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡمٞۖ وَلَا تَجَسَّسُواْ ﴾[1]، وعن معاوية بن أبي سفيان رضي الله عنه قال: سمعت رسول الله ﷺ يقول: (إنك إن اتبعت عورات الناس أفسدتهم أو كدت أن تفسدهم)[2]، وعن أبي هريرة رضي الله عنه أن رسول الله ﷺ قال: (إياكم والظن فإن الظن أكذب الحديث ولا تحسسوا ولا تجسسوا..)[3]، فحكم التجسس لا يتغير طالما يترتب عليه الإضرار بالمسلمين حيث جاء مصطلح التجسس عاما في الآيات والأحاديث وشمل كل صوره طالما كان الهدف منه هو تتبع عورات النـــاس

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وكشف أسرارهم[1].

و الشريعة الإسلامية تنظر إلى التجسس أنه من التصرفات المشينة التي تستوجب العقاب، وفي ذلك يقول ابن قدامة: "ومن اطلع في بيت إنسان من ثقبٍ أو نحوه فرماه صاحب البيت بحصاة أو طعنه بعود فقلع عينه لم يضمنها، وبه قال الشافعي"[2] واستدل على ذلك بما رواه أبو هريرة رضي الله عنه أن رسول الله ﷺ قال: (لو أن امرأ اطلع عليك بغير إذن فحذفته بحصاة ففقأت عينه لم يكن عليه جناح)[3].

وعلى ضوء ذلك فإن الذين يعتدون على بيانات الآخرين ومعلوماتهم عبر اختراق رسائلهم الإلكترونية هم آثمون لمخالفة أمر الشارع الحكيم ويستوجب عقابهم تعزيرا، وأن هذا الأمر مما استقرت الشريعة على تحريمه والنهي عنه حيث تضافرت نصوص الكتاب والسنة على حفظ حقوق الآخرين وعدم انتهاكها[4]، وقد تطرق الفقهاء إلى عقوبة الذي يتجسس على المسلمين؛ فذهب الحنفية إلى أنه يوجع عقوبة ويطال حبسه حتى يحدث توبة[5]، وذهب المالكية إلى أنه يقتل ولا يستتاب ولا دية لورثته كالمحارب لإضراره بالمسلمين وسعيه بالفساد في الأرض، وقيل : يجلد نكالاً ويطال حبسه وينفى من الموضع الذي كان فيه، وقيل: يقتل إلا أن يتوب، وقيل: يقتل إلا أن يعذر بجهل، وقيل: يقتل إن كان معتاداً لذلك[6]، وذهب الشافعية إلى أن الجاسوس المسلم يعزر ولا يجوز قتله[7]، وذهب الحنابلة إلى أن الجاسوس يقتل لضرره على المسلمين[8].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث:
جريمة صناعة المواقع الإباحية وترويجها عبر الانترنت

قال تعالى: ﴿ إِنَّ ٱلَّذِينَ يُحِبُّونَ أَن تَشِيعَ ٱلْفَٰحِشَةُ فِى ٱلَّذِينَ ءَامَنُواْ لَهُمْ عَذَابٌ أَلِيمٌ فِى ٱلدُّنْيَا وَٱلْأَخِرَةِ ۚ وَٱللَّهُ يَعْلَمُ وَأَنتُمْ لَا تَعْلَمُونَ ﴾[1].

لقد أصبح الانتشار الواسع للصور والأفلام الإباحية على شبكة الانترنت يشكل قضية ذات اهتمام عالمي[2]، حيث تشير بعض الإحصاءات أن حجم المواقع الإباحية بلغ 4.2 مليون موقع وهو ما يعادل 12 بالمائة من مجموع مواقع الانترنت، كما بلغ العدد اليومي لمتصفحي المواقع الإباحية عالميا 68 مليون متصفح أي ما يعادل 25 بالمائة من متصفحي الانترنت في اليوم، وبلغت نسبة مستخدمي الانترنت الذين يتعرضون للإعلانات الإباحية بدون إرادتهم 34 بالمائة، كما بلغ مجموع المواد الإباحية التي يتم تحميلها شهريا إلى الحواسيب الخاصة 1.5 مليار عملية تحميل وهو ما يعادل 35 بالمائة من مجموع التنزيلات شهريا، وبلغت النسبة الإجمالية لمرتادي المواقع الإباحية 42.7 بالمائة من مجموع مستخدمي الانترنت، كما قدّر مجموع متصفحي المواقع الإباحية الخاصة بالبالغين 72 مليون متصفح شهريا على مستوى العالم[3].

وتعد خطورة المواقع الإباحية وما تلحقه بالأفراد والمجتمعات من أضرار كفيلة بتحديد ضخامة المشكلة خاصة وأنها تستهدف جميع أفراد المجتمع دون مراعاة للسن أو الجنس أو الدين، حيث تشير الإحصاءات أنه بلغ مجموع الطلب اليومي على مواقع الأطفال الإباحية 116000 طلب، كما بلغ عدد المواقع الإباحية التي تَعرض الأطفال 100000 موقع ـــ علما بأن الموقع يحتوي على مئات الصفحات التي تعرض الآلاف من الصور ـــ، كما تشير الإحصاءات أيضا بأن الأطفال يتعرضون لمشاهدة المواقع الإباحية ابتداء من السن العاشرة ويتم ذلك في الغالب عن طريق الإعلانات الاقتحامية المرفقة ضمن

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المواقع المخصصة للأطفال كمواقع الألعاب الإلكترونية[1]، هذا وقد بلغ الحجم الكلي لتجارة الإباحية العالمية في سنة 2003م 57 مليار دولار، وهي إيرادات تفوق ميزانيات العديد من دول العالم[2].

المطلب الأول: مفهوم الإباحية وأثرها على الفرد والمجتمع

الفرع الأول: تعريف الإباحية في اللغة والاصطلاح

أولا ــ تعريف الإباحية في اللغة:

إِباحيّ: اسم مَنْسُوبٌ إِلَى الإِبَاحَةِ، و رَجُل إِبَاحِيٌّ: الْمُتَحَلِّلُ عَنْ كُلِّ وَازِعٍ خُلُقِيٍّ، فَلا يَتَوَرَّعُ عَن القِيَام بِأَعْمَالٍ مُنَافِيةٍ لِلأَخْلاَقِ و يَعِيشُ فِي إِبَاحِيَّةٍ : فِي فَوْضى وَلاَ يَتَقَيَّدُ بِالسُّلُوكِ وَالقَانُونِ وَالقَوَاعِدِ الأَخْلاَقِيَّةِ.

ويقال كلامٌ إباحيّ: فاحش، خارج عن حدود اللياقة والأدب مَنْ لا يتورَّع عن فعل المحظورات، المنحلّ أخلاقيًّا ويرى أن كل شيء مباحٌ له ولغيره.

والإِباحيّة: اسم مؤنَّث منسوب إلى إباحة، والإباحيَّة: فرقة تبطل قدرة الإنسان على اجتناب المنهيّات والإتيان بالمأمورات، وتنفي ملكيَّة الفرد وتشرك الجميع في الأموال والأزواج. والإباحيّة: التحلل من قيود القوانين والأَخلاق.[3]

ثانيا ــ تعريف الإباحية في الاصطلاح:

لقد اطلعت على العديد من المراجع الفقهية لكنني لم أعثر على تعريف خاص بلفظ الإباحية وقد يعود السبب في ذلك إلى حداثة الظاهرة إلا أنه يمكن تصنيفها ضمن جرائم الزنا والمجاهرة به، كما لم أحصل أيضا على تعريف لهذا اللفظ في القانون الوضعي، وحسب رأيي فإن ذلك يعود إلى اختلافات القوانين الوضعية في تحديد مفهوم الفحش الذي تتناوله المواد الإباحية، لكن ما لاحظته أنها تشترك كلها في تجريم المضمون الذي يحتوي عليه هذا اللفظ ومن بين التسميات التي لها علاقة بالإباحية في

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

القوانين الوضعية؛ المواقع غير الأخلاقية، والمواقع المخلة بالآداب العامة، ومواقع الدعارة والفجور، والمواقع الخادشة للحياء وغيرها[1].

الفرع الثاني: آثار المواقع الإباحية على الفرد والمجتمع

لقد سبق التطرق في فصل أنواع الجرائم الإلكترونية إلى حجم المسألة ومخاطرها على الأفراد والمجتمعات، كما شرحت بشيء من التفصيل مدى تأثير الظاهرة على السلوك الإجرامي ومخاطره على الفرد والمجتمع، ومن خلال ما تم طرحه يمكن استخلاص العديد من الآثار السلبية للظاهرة التي من أبرزها يلي:

1 ــ انتشار التفسخ والممارسات غير الأخلاقية ــ الفاحشة ــ في المجتمع وما ينتج عنه من أمراض خطيرة كالإيدز وغيرها.

2 ــ إغراق الضحايا خاصة الشباب منهم في مستنقعات الفاحشة، فتتعطل جهود التنمية والتقدم العلمي والحضاري، حيث أشارت بعض الدراسات العالمية أن أكثر المهتمين بالمواد الإباحية هم الشباب من الجنسين خاصة المراهقين منهم، كما تفيد الدراسات بأن 63 بالمائة من المراهقين الذين يرتادون مواقع وصور الدعارة لا يدري أولياؤهم عن الأمر شيئا، وأن أكثر مستخدمي المواد الإباحية تتراوح أعمارهم ما بين 12 و 17 سنة[2].

3 ــ الإصابة بالاضطرابات النفسية، وفقدان احترام الذات، والإحساس بالضياع والقلق والدمار النفسي.

4 ــ إضاعة الوقت في السعي وراء هذه المواد وبذل الأموال للاشتراك في المواقع الإباحية والحصول على موادها، ففي دراسة حررت لصالح البرلمان الأوروبي أنذرت بأن العولمة تسببت في انفجار تجارة الإباحية حيث تشير الدراسة أن 70 بالمائة من إجمالي الأموال التي أنفقها مواطنو الاتحاد الأوروبي على الانترنت عام 2001م ذهبت لصالح المواقع الإباحية[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

5 ــ تضرر العلاقات العائلية للمدمنين على الإباحية، إضافة إلى ظهور العدوانية والعصبية في التعامل مع أفراد العائلة وانهيار وتصدع قيم الحياة الزوجية وأسس استقرارها.

6 ــ العزوف عن الزواج والشغف بالفاحشة.

7 ــ شيوع الجرائم الجنسية وجرائم الاغتصاب، وجرائم الشذوذ الجنسي، وجرائم الاعتداء على الأطفال.[1]

ومما لاشك فيه أن هذه الأمراض ستنعكس أثارها السلبية على الجوانب الاجتماعية والاقتصادية والسياسية؛ كالتفكك الأسري، وتفشي الفقر، وارتفاع نسبة البطالة وغير ذلك من الآثار السلبية التي أصبحت تمتلئ بها أعمدة الصحف، خاصة وأن عدوى هذه المواد انتشرت في كافة أنحاء العالم بما فيها العالم الإسلامي سعيا من أصحابها إلى تحطيم القيم الدينية وإضعاف الشباب وكسر شوكتهم، والغريب في الأمر أن هؤلاء الشياطين يقفون بالمرصاد لكل من يحاول أن يحجب المواقع الإباحية، فقد نددوا بشدة ضد محاولات دول الخليج العربي لما حجبوا المواقع الإباحية من الانترنت بحجة الانفتاح والحرية حسب زعمهم[2]، مع أن حجب المواقع الضارة بالعقيدة والأخلاق من الأساليب المجدية والنافعة لصلاح الفرد والمجتمع، حيث أن النبي يوسف عليه السلام فضل السجن ليحجبه عن الفتن والإغواء ليظفر برضا الخالق سبحانه وتعالى، وقد جاء على لسانه في قول الله عز وجل:﴿ قَالَ رَبِّ ٱلسِّجۡنُ أَحَبُّ إِلَيَّ مِمَّا يَدۡعُونَنِيٓ إِلَيۡهِۖ وَإِلَّا تَصۡرِفۡ عَنِّي كَيۡدَهُنَّ أَصۡبُ إِلَيۡهِنَّ وَأَكُن مِّنَ ٱلۡجَٰهِلِينَ ﴾ [3]، فرغم كون يوسف عليه السلام من الأنبياء ومن أشد الناس طاعة لله وأكثرهم عبادة له، لم يأمن على نفسه من الفتنة الحاضرة غير المحجوبة ولا الممنوعة، فدعا ربه أن يحجب هذا الشر عنه فاستجاب الله لدعائه.

وإضافة إلى ما تم ذكره من الآثار السلبية لظاهرة المواقع الإباحية فإن آثارها على صحة ونفسية الفرد أشد، حيث نشرت دراسة علمية حديثة أجريت من قبل باحثين في جامعة كامبردج[4]

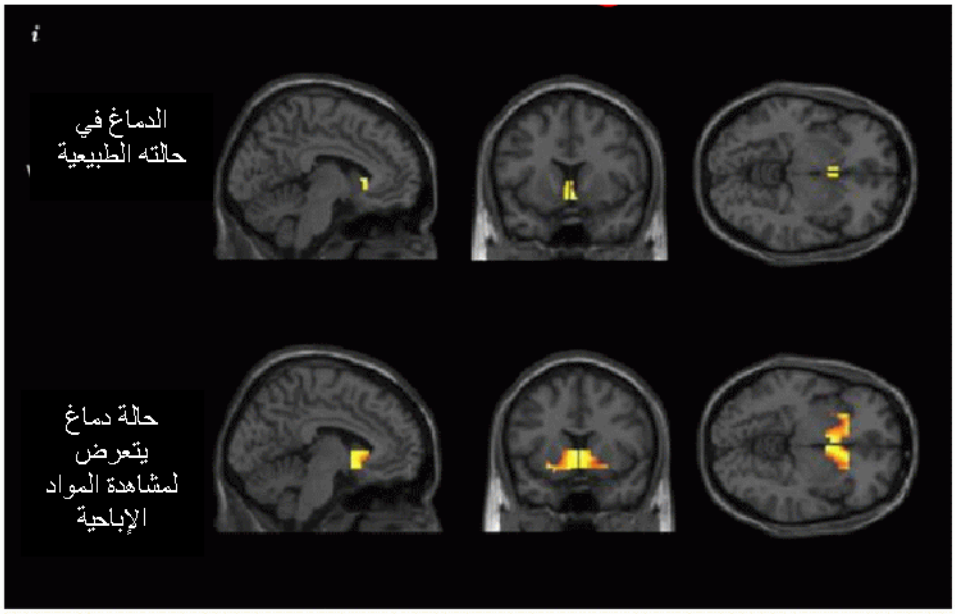
---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

Cambridge University اكتشف فيها أن دماغ الإنسان الذي ينظر للمحرمات وبخاصة المقاطع الإباحية فإنه يسلك سلوكاً يشبه دماغ الذي يدمن المخدرات والخمر، فصرحت الدكتورة Valerie Voon بحدوث نشاط هائل في منطقة من الدماغ تدعى ventral striatum وهي المنطقة المسؤولة عن المكافأة والتحفيز والسعادة، فبمجرد النظر لمشهد جنسي يزداد على الفور إفراز مادة السيروتونن Serotonin ومادة الدوبامينDopamine والأكسيتوسين Oxytocin فيتشكل فيضاناً يجتاح الدماغ ويكون له أثر سلبي على العديد من المهام كعمليات التذكر والتعلم.. و قد تتعرض أجزاء من خلايا الدماغ إلى التلف![1].



شكل رقم (33): يبين الصور الناتجة عن المسح المغناطيسي للمنطقة المسؤولة عن المكافأة في الدماغ حيث يظهر عليها نشاط غير عادي أثناء رؤية المشاهد الإباحية، وهو ما يفسر أن تكرار هذه المشاهد يؤثر على الدماغ وينهكه تماماً بنفس تأثير الإدمان على المخدرات والخمر حسب الدراسة[2]

و الدوبامين Dopamine هي مادة يفرزها الدماغ ليشعر الإنسان بالسعادة أثناء حصوله على المال أو عندما ينجز عملاً ناجحاً على سبيل المثال، لكن عندما يدمن الدماغ على مشاهدة المناظر

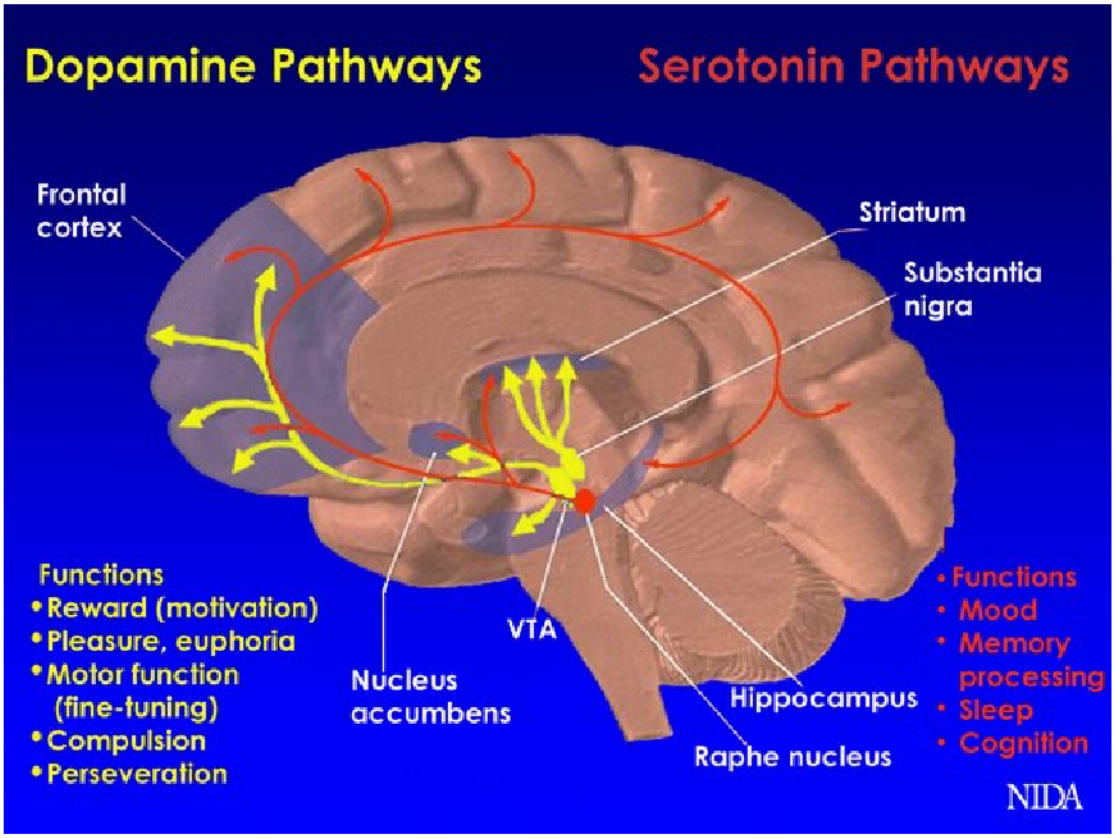
---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

الجنسية فإنه يكثر من إفراز هذه المادة، وبمرور الوقت تتعب الخلايا المسؤولة عن إفرازها فتضعف وتضمر تدريجياً.. وهو ما يجعل المدمن على الإثارة يفقد الشعور بالسعادة كما كان من قبل، فيبدأ بالبحث عن وسائل أشد إثارة ـــ وهو ما يحصل لمدمن المخدرات ـــ وبالتالي يزداد الضرر ويزداد تلف الخلايا وتدميرها..! كما تمتد الأضرار أيضا إلى منطقة الناصية[1] من الدماغ حيث تتأذى وتتآكل تدرجياً فيفقد صاحبها القدرة على اتخاذ القرارات الصائبة.



شكل رقم(34): يوضح مسار ومهام مادتي Dopamine ، وSerotonin في دماغ الإنسان[2]

ولقد أكد الدكتور Norman Doidge في كتابه The Brain That Changes Itself أن المشاهد الإباحية تحدث تغييرات خطيرة في الدماغ، وتجعل من اعتاد على مشاهدتها في حالة استنفار دائم وإدمان على المشاهدة من دون سبب، مما يزيد احتمال ارتكابه لجرائم الاغتصاب والزنا بنسب كبيرة جداً[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما لوحظ على مدمني مشاهد الإباحية حصول زيادة مفرطة في إفرازات مادة الأوكسيتوسين Oxytocin وهي المسؤولة عن الثقة بين البشر ومنها الثقة بين الزوجين، ولما يتشكل لدى المدمنين ما يسمى بالعشق الافتراضي يختل إفراز هذه المادة ويختل معها إفراز بعض الهرمونات.. وكنتيجة لذلك تتضرر الحياة الاجتماعية للمدمنين، فيتأثر سلبا الرباط الأسري وما ينجر عنه من أضرار[1].

الفرع الثالث: حكم صناعة المواقع الإباحية وترويجها

إن الزنا هو من أبشع الجرائم المحرمة في الشريعة الإسلامية حيث قال تعالى:﴿ وَلَا تَقْرَبُواْ ٱلزِّنَىٰٓ إِنَّهُۥ كَانَ فَٰحِشَةً وَسَآءَ سَبِيلًا ﴾[2]، وقد شرعت في ذلك عقوبات تصل إلى حد الرجم حتى الموت نظرا لما تؤول إليه هذه الجريمة من آثار سيئة على الفرد والمجتمع ومنافاتها للضرورات الخمس.

ولقد حرّم الشارع الحكيم كل ذريعة تؤدي إلى جريمة الزنا ككشف العورات والاختلاء بالأجنبيات والاختلاط غير المشروع، وما ارتياد المواقع الإباحية إلا من المحظورات الشرعية التي حرص الشارع الحكيم على التنبيه عليها وتحريمها، فقد أمرنا الله عز وجل بغض البصر وحرّم النظر إلى الأجنبيات بأي صورة كانت، فقال سبحانه وتعالى في سورة النور:﴿ قُل لِّلْمُؤْمِنِينَ يَغُضُّواْ مِنْ أَبْصَٰرِهِمْ وَيَحْفَظُواْ فُرُوجَهُمْۚ ذَٰلِكَ أَزْكَىٰ لَهُمْۗ إِنَّ ٱللَّهَ خَبِيرُۢ بِمَا يَصْنَعُونَ ﴾[3]، وقال عز وجل:﴿ وَلَا تَقْرَبُواْ ٱلْفَوَٰحِشَ مَا ظَهَرَ مِنْهَا وَمَا بَطَنَۖ ﴾[4]، وفي ذلك حرّم رسول الله ﷺ أن تصف المرأة لزوجها جمال امرأة أخرى لا تحل له وكأنه ينظر إليها، قَالَ النبي ﷺ : (لا تُبَاشِرُ الْمَرْأَةُ الْمَرْأَةَ فَتَنْعَتَهَا لِزَوْجِهَا كَأَنَّهُ يَنْظُرُ إِلَيْهَا)[5]، وقال ﷺ: (العينان تزنيان وزناهما النظر)[6].

وإن من حكمة الشارع الحكيم ومعرفته بالغرائز البشرية التي يساهم الشيطان في تأجيجها ليوقع الإنسان في جريمة الزنا، فقد حرّم الاقتراب منه في قوله تعالى:﴿ وَلَا تَقْرَبُواْ ٱلزِّنَىٰٓ إِنَّهُۥ كَانَ فَٰحِشَةً وَسَآءَ

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

سَبِيلًا ﴾ [1]، ويقول القرطبي رحمه الله في تفسير هذه الآية: " قال العلماء قوله تعالى: ﴿ وَلَا تَقْرَبُواْ ٱلزِّنَىٰٓ ﴾ أبلغ من أن يقول ولا تزنوا، فإن معناه فلا تدنوا من الزنا، فأي اقتراب من المحظور هو فعل محظور في حد ذاته"[2]، ومن ذلك مشاهدة المواد الإباحية فضلا عن الاشتراك في المواقع الإباحية أو شراء مواد جنسية منها، أو إنتاجها ونشرها وهو الأخطر ضررا لأن هذا التصرف يتعدى ضرره للغير ويدخل فاعله في وعيد الله عز وجل، حيث قال جل وعلا في سورة النور: ﴿ إِنَّ ٱلَّذِينَ يُحِبُّونَ أَن تَشِيعَ ٱلْفَٰحِشَةُ فِى ٱلَّذِينَ ءَامَنُواْ لَهُمْ عَذَابٌ أَلِيمٌ فِى ٱلدُّنْيَا وَٱلْءَاخِرَةِ ۚ وَٱللَّهُ يَعْلَمُ وَأَنتُمْ لَا تَعْلَمُونَ ﴾ [3]، فالأضرار التي تنجم عن جريمة إنتاج ونشر المواقع الإباحية تجعلها أقرب إلى جريمة الحرابة، وإن كانت تعني عند أكثر الفقهاء الخروج لأخذ المال أو قتل الأنفس أو إرهاب المارة اعتمادا على القوة[4]، فإنها تعني عند المالكية حالات أخرى غير سلب المال مثل حالات المغالبة على الفروج أي الاغتصاب وانتهاك الأعراض، حيث يقول ابن العربي المالكي: " ألم تعلموا أن الحرابة في الفروج أفحش منها في الأموال، وأن الناس يرضون أن تذهب أموالهم وتخرب من أيديهم، ولا يرضون أن يعتدى على زوجاتهم وبناتهم، ولو كان فوق ما قال الله عقوبة لكانت لم يسلب الفروج"[5].

كما أن الذين يعملون على إنتاج ونشر الفاحشة والفساد هم يحاربون الله بمعاداتهم للدين الإسلامي وقيمه، والله سبحانه وتعالى يقول:﴿ إِنَّمَا جَزَٰٓؤُاْ ٱلَّذِينَ يُحَارِبُونَ ٱللَّهَ وَرَسُولَهُۥ وَيَسْعَوْنَ فِى ٱلْأَرْضِ فَسَادًا أَن يُقَتَّلُوٓاْ أَوْ يُصَلَّبُوٓاْ أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُم مِّنْ خِلَٰفٍ أَوْ يُنفَوْاْ مِنَ ٱلْأَرْضِ ۚ ذَٰلِكَ لَهُمْ خِزْىٌ فِى ٱلدُّنْيَا ۖ وَلَهُمْ فِى ٱلْءَاخِرَةِ عَذَابٌ عَظِيمٌ ﴾ [6]، وهي آية مناسبة لأن تكون مصدرا لتشريع عقوبة محددة للضرب على أيدي المجرمين الذين يعملون على إثارة الفتن ونشر الدعارة والتحريض عليها، والتي من شأنها إفساد النسل والأمن العام داخل المجتمع الإسلامي وهذا باعتبارها جرائم تتفق في المآل مع جريمة الحرابة[7].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وعلى ضوء ما سبق فإن ارتياد المواقع الإباحية أو الإدمان عليها محرم شرعا بالنص الصريح في قوله تعالى:﴿ قُل لِّلْمُؤْمِنِينَ يَغُضُّواْ مِنْ أَبْصَٰرِهِمْ وَيَحْفَظُواْ فُرُوجَهُمْ ذَٰلِكَ أَزْكَىٰ لَهُمْ إِنَّ ٱللَّهَ خَبِيرٌۢ بِمَا يَصْنَعُونَ ﴾[1]، فتستوجب عقوبات تعزيرية مشددة لأن ارتيادها سيكون حتما ذريعة لاقتراف جرائم أشد على الفرد والمجتمع، كما أضم رأيي إلى المذهب المالكي في اعتبار صناعة المواد الإباحية ونشرها هي من باب المغالبة على الفروج والمجاهرة على الاغتصاب وانتهاك الأعراض والتي تستوجب حد الحرابة الذي تدور عقوبته وفق ما تبينه الآية في قوله تعالى:﴿ إِنَّمَا جَزَٰٓؤُاْ ٱلَّذِينَ يُحَارِبُونَ ٱللَّهَ وَرَسُولَهُۥ وَيَسْعَوْنَ فِى ٱلْأَرْضِ فَسَادًا أَن يُقَتَّلُوٓاْ أَوْ يُصَلَّبُوٓاْ أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُم مِّنْ خِلَٰفٍ أَوْ يُنفَوْاْ مِنَ ٱلْأَرْضِ ﴾[2].

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفصل الثالث:
جرائم التعدي على أمن الدولة والمجتمع

المبحث الأول: جرائم التجسس الإلكتروني.

المبحث الثاني: جريمة غسيل الأموال عن طريق الانترنت

المبحث الثالث: جرائم الإرهاب الإلكتروني

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الأول: جرائم التجسس الإلكتروني

لقد ساهمت التكنولوجيا الحديثة وخصوصا منها الانترنت إلى اتساع نشاط التجسس لما تتيحه من تسهيلات مقارنة بالطرق والوسائل التقليدية، وقد عرف التجسس الإلكتروني انتشارا واسعا بين مختلف فئات المجتمع سواء محترفين أو هواة أو فضوليين وهو ما انعكس سلبا على حقوق وخصوصيات الآخرين وأسرارهم، كما اقتضى التنافس الدولي إلى محاولة كل دولة الاطلاع على أسرار غيرها والتعرف على أحوالها وأخبارها وثرواتها العلمية وقدراتها العسكرية.. إلى جانب محاولة حماية ذاتها من التمرد والمؤامرات مسخرة في ذلك وسائل التقنية الحديثة وأساليبها وبذلك اتخذ التجسس صورا جديدة أشد ضراوة من السابق.

ولقد كفلت الشريعة الإسلامية حفظ الحقوق العامة والخاصة وحرّمت الاعتداء عليها بغير حق وبأي طريقة كانت، ومن أوجه الاعتداء التجسس غير المشروع، فإذا كان ديننا الحنيف ينهى كل مسلم عن التعدي على حقوق الآخرين فإن التجسس الإلكتروني بالمفهوم الشائع من حيث هو سطو على نتاج جهد الآخرين يكون على رأس قائمة المحظورات الواجب الالتزام بها، وإن كان الوجه الآخر لهذا الموقف أن نعد لأعدائنا ما استطعنا من القوة وأن نتسلح بالفطنة والكياسة، وأن نغلق كل ثغرة يمكن أن ينفذ منها العدو للإضرار بحقوق أمتنا.

المطلب الأول: مفهوم التجسس الإلكتروني

الفرع الأول: تعريف التجسس في اللغة

التجسس لغة: من الجس، والجس: اللمس باليد وموضعه المجسة، يجسه جسًا، واجتسه أي: مسه ولمسه، وجس الشخص بعينيه إذا أحدّ النظر إليه ليستبينه ويثبته وهو مجاز حيث إن الجس هو اللمس باليد باعتبار ما فيه من معنى الطلب باللمس، فإن من يطلب شيئا يجسه ويلمسه، فأريد ما يلزمه، واستعمل التفعل للمبالغة، ومنه جس الأرض جسًا: وطئها[1].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وجس الخبر: بحث عنه، وتفحص، وتجسس الأمر إذا تطلبه وبحث عنه، ومنه: التجسس. يقال: تحسست الخبر، وتجسسته بمعنى واحد: لتقاربهما فليس يتعدى إحداهما من الأخرى، لأن التجسس: البحث عما يكتم والتحسس (بالحاء المهملة) طلب الأخبار والبحث عنها، ويقال: تجسس الأمر إذا تطلبه وبحث عنه على وزن: "تفعل" كما أن التطلب من اللمس، لما في اللمس من الطلب، وقد جاء بمعنى الطلب في قوله تعالى: ﴿ وَأَنَّا لَمَسْنَا ٱلسَّمَآءَ ﴾[1] فالمعنيان متحدان إذ مآلهما واحد، وهو معرفة الأخبار[2]. وقيل التجسس بالجيم: البحث عن العورات، وبالحاء الاستماع إلى حديث القوم وهم له كارهون[3].

الفرع الثاني: تعريف التجسس في الاصطلاح الفقهي

لم يرد في الكتب الفقهية التي اطلعت عليها أي تعريف اصطلاحي حول لفظ التجسس، وقد يعود السبب في ذلك إلى ظهور معناه فكان كافيا للدلالة عليه دون تحديد ألفاظه، خاصة وأن لفظ التجسس ورد صراحة في القرآن الكريم في معرض النهي عنه وذلك في قوله تعالى:﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجْتَنِبُواْ كَثِيرًا مِّنَ ٱلظَّنِّ إِنَّ بَعْضَ ٱلظَّنِّ إِثْمٌ وَ لَا تَجَسَّسُواْ وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَٱتَّقُواْ ٱللَّهَ إِنَّ ٱللَّهَ تَوَّابٌ رَّحِيمٌ ﴾[4]، وهو نهي موجه إلى آحاد المسلمين وجماعاتهم بمعنى: ولا تبحثوا عن عورات المسلمين وعيوبهم، وتستكشفوا عما ستر الله تعالى، كما قرئ لفظ التجسس أيضا بالحاء المهملة (ولا تحسسوا) من الحس الذي هو أثر الجس وغايته، والمراد على القراءتين: النهي عن تتبع العورات مطلقا، ويعد من الكبائر[5].

كما ورد التجسس صراحة في قوله ﷺ: (إياكم والظن فإن الظن أكذب الحديث، ولا تحسسوا، ولا تجسسوا، ولا تناجشوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا، وكونوا عباد الله إخوانا)[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وقد ذكر الجاسوس في معظم كتب الفقه بمعنى العين وأن العين هو الجاسوس[1]، كما ورد معناه بأنه: " الشخص الذي يطلع على عورات المسلمين، وينقل أخبارهم للعدو"[2].

ويعرّف الجاسوس حديثا بأنه: الشخص الذي يطلع على عورات المسلمين بطريقة سرية، وينقل أخبارهم للعدو سواء أكان هذا الشخص مسلما أم غير مسلم، وسواء أكانت هذه الأخبار عسكرية أم غير عسكرية، في وقت السلم أو في وقت الحرب[3].

المطلب الثاني: أنواع التجسس وأحكامه

يُعرف في الشريعة الإسلامية نوعان من التجسس؛ التجسس المشروع والغير مشروع وبيانهما كما يلي:

الفرع الأول: التجسس المشروع

أجاز الفقهاء التجسس على اللصوص وقطاع الطرق، وطلبهم عن طريق التجسس عليهم وتتبع أخبارهم[4]، كما يجوز التجسس في حال الحرب بين المسلمين وغيرهم لمعرفة أخبار جيش الكفار وعددهم وعدتهم وكل ما له صلة بذلك. فقد عرف عن غزوات الرسول ﷺ والتي انتصر فيها المسلمون في الجزيرة العربية وخارجها استعمال كافة الوسائل العسكرية المعروفة في ذلك الوقت بما في ذلك التجسس لما له من أهمية في الحصول على المعلومات المتعلقة بالعدو والتي بدورها تعد سلاح قوي في الحرب خاصة فيما يتعلق بالتخطيط والإعداد[5].

ولقد جاء عن أبي هريرة رضي الله عنه أنه بعث ﷺ عشرة عينًا في غزوة بدر يتجسسون له[6]. ولما أمر رسول الله ﷺ بتجهيز جيش أسامة بن زيد رضي الله عنه قال له: (يا أسامة: سر على اسم الله، وبركته، حتى تنتهي إلى مقتل أبيك، فأوطئهم الخيل، فقد وليتك هذا الجيش، فأغر صباحا على

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أهل أبنا ـــ أبين ـــ[1] وحرّق عليهم وأسرع السير تسبق الأخبار، فإن أظفرك الله، فأقلل اللبث فيهم وخذ معك الأدلاء وقدم العيون أمامك والطلائع)[2].

كما ثبت أن للرسول ﷺ عيون محلية في المدينة المنورة، وعيون في مكة المكرمة يطلعونه على كل صغيرة وكبيرة قد تضر بمصلحة المسلمين في السلم والحرب، ففي مكة المكرمة كان العباس بن عبد المطلب عم النبي ﷺ يأتيه بالأخبار، حيث أرسل له العباس بوقت خروج قريش لقتاله في أُحد كما أعلمه بعدد قواتها، وقد كان العباس يرغب في الهجرة إلا أن الرسول ﷺ كتب إليه : (إن مقامك في مكة خير)[3].

وقد كان النبي ﷺ يحرص ألا تتسرب الأخبار إلى العدو فعمل على مقاومة جواسيس قريش في مكة والمدينة فبث ﷺ عيونه ودورياته لتجوس الدروب حول المدينة كي تحول دون تسرب المعلومات إلى قريش، كما بث عيونه في الداخل ليقضي على كل خبر يمكن أن يصل أو يتسرب إلى قريش عن طريق عيونها داخل صفوف المسلمين وذلك في فتح مكة في السنة الثامنة للهجرة، وكل ذلك ليتمكنﷺ من السيطرة على الموقف وليستفيد من عنصر المبادرة أيضا[4]. ولإدراكه ﷺ بخطورة علم العدو بتحركات المسلمين دعا ربه قائلا: (اللهم خذ العيون والأخبار عن قريش حتى نبغتها في بلادها)[5].

وفي عصرنا يعد التجسس أحد الضمانات الأساسية لبقاء الدولة واستقلالها، فنتيجة لتضارب المصالح وتعدد الأفكار واختلاف الأغراض كان لزاما على الدولة أن تكون متأهبة في كل لحظة لمواجهة أي عدوان قد يشن عليها مستغلة في ذلك كل الوسائل والطرق المتاحة ومن بينها التجسس الإلكتروني، لأن مستقبل الدولة في هذا العصر خاصة يتوقف على دقة المعلومات التي تحصل عليها

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وشمولها وسرعة وصولها ليتسنى وضع الخطة المناسبة بعد معرفة خطة العدو وحالته حيث إن مصيرها إما مغلوبة أو منتصرة[1].

وما يجب التنويه له، أن التجسس المشروع هو من صلاحيات ولي الأمر ـــ الدولة النظامية ـــ ولا يتم إلا بكيفيات تتماشى وفق الضوابط الشرعية التي أمر بها الشارع الحكيم، ومن أبرز صوره:

ـــ التجسس على الأفراد والجماعات للتعرف على طاقاتهم من أجل الاستعانة بهم والأخذ بمشورتهم في تصريف شؤون الدولة خدمة للمصلحة العامة؛ فمن واجب ولي الأمر أن يعرف قدرات المواطنين وذوي الخبرة وأهل الحل والعقد لأنه مأمور أن يحكم الناس بالعدل، ولابد من وجود بطانة تساعده في إدارة دفة الحكم وله أن يفاضل بين الناس ويدرس حياتهم ليضع له بطانة صالحة، وفي ذلك يقول ﷺ: (ما بعث الله من نبي ولا استخلف خليفة إلا كانت له بطانتان: بطانة تأمره بالمعروف وتحضه عليه، وبطانة تأمره بالشر وتحضه عليه والمعصوم من عَصَمَ الله تعالى)[2].[3]

ـــ التجسس على أهل الريب والمجرمين وتعقبهم والوقوف على حال الرعية؛ فالدولة مكلفة بحماية أفرادها والمقيمين فيها انطلاقا من أهداف الإسلام السامية في إقرار المبادئ الإنسانية والسلام في العلاقات الاجتماعية، وعلى الدولة أن تحقق العدالة الاجتماعية وأن تتعقب المجرمين وتدرأ شرهم وخطرهم وأذاهم ليعيش الناس آمنين من إفسادهم، ولتحقيق ذلك لابد لها من مراقبة دقيقة تقوم بها الدولة لتهيئة جو من الأمن والاستقرار في المجتمع، ولابد من وجود أجهزة خاصة لذلك[4].

وقد اتخذ الرسول ﷺ الأعوان والمساعدين لتحقيق الأمن وحماية المجتمع من خطر المنافقين وأهل الريب والسوء، قال أبو الدرداء: " ألم يكن فيكم صاحب الوساد وصاحب السر الذي لا يعلمه غيره والذي أجير من الشيطان على لسان النبي ﷺ ؟ أما صاحب الوساد: ابن مسعود، وصاحب السر: حذيفة، والذي أجير من الشيطان: عمار"[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ التجسس على العدو؛ فمن ضرورات بقاء الدولة وحمايتها أن لا يغفل الحاكم عن بث الجواسيس على أعدائه، ورصد تحركاتهم، ومعرفة نواياهم وأسرارهم، مع الحذر الدائم لأن العدو يتحين له غفلة ليتمكن منه في غرة ولذلك يجب أن لا يستهان بالعدو مهما كان ضعيفا[1].

وبناء على ذلك فإن صور التجسس المشروع إذا تمت عن طريق الوسائل الإلكترونية الحديثة، وكانت صادرة من ولي الأمر وقائمة على الضوابط الشرعية ومقاصد الشريعة الإسلامية فإن حكمها الجواز.

الفرع الثاني: التجسس غير المشروع

لقد نهى الله سبحانه وتعالى عن التجسس نهيا عاما، ويدخل في ذلك كل أنواع التجسس المتعلقة بالفضول أو كشف العورات، أو خدمة جهة من الجهات على سبيل الخيانة والإضرار بالغير، ويشمل الحاكم والمحكوم لأن الخطاب موجه للجميع، وتفصيل ذلك كما يلي[2]:

أولاـــ التجسس على العورات:

أجمع العلماء على تحريم التجسس بغرض فضح عورات المسلمين أو الذميين بأي صفة كانت، وذلك لقوله تعالى:﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجْتَنِبُواْ كَثِيرًا مِّنَ ٱلظَّنِّ إِنَّ بَعْضَ ٱلظَّنِّ إِثْمٌ وَ لَا تَجَسَّسُواْ وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَٱتَّقُواْ ٱللَّهَ إِنَّ ٱللَّهَ تَوَّابٌ رَّحِيمٌ ﴾[3]، فالآية تنهى صراحة عن التجسس وتتبع عورات وعيوب المسلمين والكشف عما ستره الله تعالى، كما يحرم أيضا التجسس على الذميين تبعا لهذا القصد، وقد اعتبر بعض العلماء التجسس من الكبائر[4].

وقد ورد عن النبي ﷺ أنه قال: (إياكم والظن فإن الظن أكذب الحديث ولا تجسسوا ولا تحسسوا ولا تناجشوا ولا تحاسدوا ولا تباغضوا ولا تدابروا وكونوا عباد الله إخوانا)[5]، ووجه الاستدلال من الحديث، أن التجسس المفضي إلى فضح عورات الناس حرام، وعلى المسلمين أن يأخذوا بما ظهر ولا يتبعوا ما بطن من عورات إخوانهم سواء أكانـــوا أفرادا أم جماعـــات، وفي ذلك

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

قالﷺ : (من ستر عورة مؤمن فكأنما استحيا موؤدة من قبرها)[1].

ولذلك لا يجوز التجسس ابتداء ولو من الحاكم ما لم تظهر الشبهة أو خبر الثقة لتدارك حرمة ما، كما لا يجوز التنصت[2] على سرائر الناس سواء أكان من باب الفضول لدى العامة أم من الحاكم إلا في حالة ظهور أمارة دالة على ارتكاب محظور[3]، ومثال ذلك في الجرائم الإلكترونية؛ لو ظهرت أمارة تدل على أن شخص ما يتاجر بالمواقع الإباحية سواء كان ينتجها أو يصممها أو يسير مبيعاتها فإنه من حق الحاكم أن يأمر بالتجسس على نشاطه الإلكتروني لإثبات التهمة وتوقيف الجاني حفاظا من انتهاك الحرمات وارتكاب المحظورات.

وقد روي عن عمر بن الخطاب رضي الله عنه أنه دخل على قوم يتعاقرون على شراب ويوقدون في أخصاص[4] فقال: "قد نهيتكم عن المعاقرة فعاقرتم، ونهيتكم عن الإيقاد في الأخصاص فأوقدتم؟ فقالوا: يا أمير المؤمنين قد نهاك الله عن التجسس فتجسست، ونهاك عن الدخول بغير إذن فدخلت فقال عمر: هاتان بهاتين وانصرف"[5]. فالأصل أن من أغلق باب داره وتستر بحيطانه، لا يجوز التجسس عليه لضبط ما هو واقع فيه من منكر، أما إذا ارتكب المنكر داخل الدار وظهرت أمارات عليه في خارج الدار كظهور رائحة الخمر وأصوات السكارى فإنه يجوز للمحتسب الدخول على المترل وتفتيشه للقضاء على المنكر المتلبس به، لأن النصوص الواردة في النهي عن التجسس خاصة بمن لم يجاهر بمعصيته، وأما من جاهر بالمعصية ـــ مثل الذي ينشر المواقع الإباحية ـــ فإنه لا يشمله هذا الفضل نظرا لما يصدر عنه من أمور تخالف الشرع، فالمجاهر قد ينتج عن فعله ترويج الفاحشة وفعل المنكرات في المجتمع المسلم، ودرء المفاسد مقدم على جلب المصالح، كما أن المصلحة العامة مقدمة على المصلحة الخاصة[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وقصة عمر بن الخطاب رضي الله عنه تدل على أنه لا يجوز تتبع عورات المسلمين، وأن يأخذ الناس بما ظهر دون التجسس أما التجسس ابتداء فإنه لا يجوز، وفي حالة الأمر بالمعروف والنهي عن المنكر يقول بعض المالكية: " يشترط أن يكون الآمر بالمعروف والناهي عن المنكر عالما بهما، ويشترط ظهور المنكر من غير التجسس ولا استراق سمع، ولا استنشاق ريح، ولا بحث عما أخفي بيد أو ثوب أو حانوت فإنه حرام"[1].

ثانيا ــ التجسس لصالح العدو:

إن الذين يتجسسون لصالح أعداء أمتهم يتجاوزون في عملهم كل عرف وخلق، فهم من الذين خرجوا عن طاعة الله ولا يهمهم إلا هزيمة المسلمين ونصرة العدو ولا يتوانون بإبلاغه بخطط المسلمين وأخبارهم، مع أن الله عز وجل قد نهى عن ذلك في قوله تعالى: ﴿يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَتَّخِذُواْ ٱلْيَهُودَ وَٱلنَّصَـٰرَىٰٓ أَوْلِيَآءَ ۘ بَعْضُهُمْ أَوْلِيَآءُ بَعْضٍ ۚ وَمَن يَتَوَلَّهُم مِّنكُمْ فَإِنَّهُۥ مِنْهُمْ ۗ إِنَّ ٱللَّهَ لَا يَهْدِى ٱلْقَوْمَ ٱلظَّـٰلِمِينَ ﴾[2]، وقد جعل الله ما يعلمه الإنسان من حديث أخيه الإنسان أمانة يستوجب الحفاظ عليها وعدم خيانتها في قوله تعالى:﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَـٰنَـٰتِكُمْ وَأَنتُمْ تَعْلَمُونَ ﴾ [3]، والعبرة بعموم اللفظ لا بخصوص السبب.

كما نهى النبي ﷺ المسلمين من أن يخذلوا بعضهم بعضا في قوله ﷺ: (ما من امرئ يخذل امرأ مسلما في موضع تنتهك فيه حرمته، وينتقص فيه من عرضه إلا خذله الله تعالى في موطن يحب فيه نصرته، وما من امرئ ينصر امرأ مسلما في موضع ينتقص فيه من عرضه وينتهك فيه من حرمته إلا نصره الله عز وجل في موطن يحب فيه نصرته)[4]، وفيما يرويه جابر بن عبد الله قال: قال رسول الله ﷺ : (إذا حدث الرجل بالحديث ثم التفت فهي أمانة)[5] والأمانة لا يجوز إضاعتها بإشاعتها، ولذلك فإن التجسس على المسلمين وإعطاء العدو معلومات عنهم بأي طريقة كانت هي خيانة لله وللرسول وللمؤمنين[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ثالثا ــ التجسس المزدوج:

التجسس المزدوج يكون لحساب فئتين مختلفتين وهي من أخطر صور التجسس ضررا، فالذين يقومون بمثل هذا العمل يسعون من وراءه إلى نشر الفتن والحروب كما يسعون لهثا وراء مغانم ومطامع مادية فيبيعون الأخبار لمن يدفع لهم المال، وقد يصدقون وقد يكذبون، كما يصدقون مع دولة ويخدعون أخرى[1]، ولذلك فإن المسلم إذا أعطى الولاء لغير المسلمين فإنما يكون منافقا خالصا لأن العداوة والبغضاء، والصداقة، والود، والكراهية لا تجتمع في قلب واحد في زمان واحد لجهة واحدة[2].

المطلب الثالث: حكم التجسس الإلكتروني في الفقه الجنائي الإسلامي

بناء على ما تقدم ذكره نخلص إلى أن التجسس محرم شرعا إلا ما استثني منه في الشريعة الإسلامية، وهو ما ينطبق أيضا على التجسس الإلكتروني لأن الحكم الشرعي يقع على الغاية المتوصل إليها دون أن يحدد الوسيلة المستعملة في ذلك، فاستعمال أي وسيلة بغرض التجسس على الغير سواء كانت تقليدية أم حديثة فذلك لا يغير من الحكم شيئا، شأن ذلك شأن جريمة القتل العمدي فإن عقابها لا يختلف عن القتل بالسلاح الأبيض أو الرصاص أو أي وسيلة كانت.

ولذلك فإن الشريعة الإسلامية كفلت حفظ الحقوق الشخصية للإنسان وحرمت الاعتداء عليها بغير حق، فالذين يتجسسون على بيانات الآخرين ومعلوماتهم عبر اختراق بريدهم الإلكتروني أو حواسيبهم أو مواقعهم الإلكترونية ونحوها هم آثمون لمخالفة ما أمر به الله سبحانه وتعالى ومستحقون للعقاب الشرعي، وهو حكم يجب إشاعته في المجتمع الإلكتروني الإسلامي وتوعية المتعاملين بالشبكة العالمية بخطورة انتهاك خصوصية الآخرين وأن الشريعة الإسلامية استقرت على تحريمه والنهي عنه.

ولقد شددت الشريعة الإسلامية على معاقبة المتجسسين على المسلمين سواء كان الجاسوس مسلما أو معاهدا أو حربيا وذلك كما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الأول: عقوبة الجاسوس المسلم

جاء الفقهاء في عقوبة الجاسوس المسلم على أمته بثلاثة آراء تدور بين القتل والتعزير، فإذا خدم الأعداء بدافع الإخلاص لهم واستهتر بحق المسلمين ومصيرهم فإنه يجوز للإمام أن يأمر بقتله تعزيرا له ليكون عبرة لغيره، وذلك إذا كان ميئوس منه فيُعد في حكم المرتد ما لم يحدث توبة صادقة ويكون تصرفه زلة عارضة، لأن الجاسوس يضر بمصلحة الأمة وقد يحدث بسببه قتل الكثير من المسلمين، وقتل الجاسوس في هذه الحالة هو من العقوبات التعزيرية الموكلة إلى الإمام صاحب السلطة الشرعية فله أن يتركه بالتوبة ويكتفي بتعزيره بما هو أخف من القتل كالجلد والسجن على حسب ما أفضى به جرمه وذلك لاعتبارات يراها الإمام ويقدرها سياسة ومن بينها الإسلام[1].

الفرع الثاني: عقوبة الجاسوس غير المسلم

يكون الجاسوس من غير المسلمين إما ذميا، أو مستأمنا، أو محاربا، وعقابهم كما يلي[2]:

أولا ــ الجاسوس الذمي[3]: وفي حكمه ثلاثة آراء؛ ينتقض عهده ويخرج من ذمته ويخير فيه الإمام بين القتل أو الصلب أو الاسترقاق، وبه قال مالك والأوزاعي والإمام أحمد في الراجح عنده وأبو يوسف[4]، ويقضي الرأي الثاني بعدم قتله ولا ينتقض عهده بالتجسس إلا أن يكون شرط عليه ذلك وهو ما قال به أكثر الشافعية ورجحه الحنابلة[5]، والرأي الثالث يوجع الجاسوس عقوبة[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والراجح؛ أنه ما دامت عقوبة المسلم قد تصل إلى حد القتل فإنه يجوز للإمام أن يقتل الجاسوس الذمي سياسة شرعية، لأن التعزير يكون في حق المسلمين دون غيرهم ولذلك على الإمام قتل الجاسوس الذمي إن رأى ذلك مناسبا وفق ظروف الجريمة وجسامتها وخطورتها على الإسلام والمسلمين[1].

ثانيا ــ الجاسوس المستأمن[2]: بيّن الفقهاء أن المستأمن لو دخل دار الإسلام بأمان لمدة محددة وكان قد شرط عليه عدم التجسس على عورات المسلمين أو الدلالة على عوراتهم بالمكاتبة أو غيرها فإنه ينتقض عهده بذلك اتفاقا[3]، واختلف الفقهاء فيما لو لم يشترط عليه ذلك أن يعاقب بالقتل أو التنكيل والحبس.

فالمستأمن ليس مواطنا مقيما في الدولة الإسلامية بل أعطى الأمان وهو ما يقابل تأشيرة الدخول الدالة على الأمان والموافقة على وجوده في البلاد لمدة معينة، ولذلك فإن الشرط الضمني لدخول المستأمن أرض الإسلام يتضمن ترك كل ما فيه ضرر على أمن الدولة وسلامتها وسلامة المواطنين وآحادهم من مال أو نفس أو عرض وغيره سواء شرط عليه ذلك في العقد أو لا، لأن في الأصل لا يسمح له لو عُلم بضرره.

وفي حال تعديه فإن للإمام أن يسحب الأمان منه عقوبة له، ويأمره بمغادرة البلاد، وله أن يأمر بسجنه أو ضربه لاستنطاقه، وله أن يأمر بقتله وذلك حسب جسامة الجرم وخطورته[4].

ثالثا ــ الجاسوس الحربي: اتفق الفقهاء على قتله[5] بباعث اطلاعه على عورات المسلمين ومبادرته بإعلام أصحابه، ولذلك كان في قتله مصلحة المسلمين لأن تجسس الحربي عليهم أشبه بمقاتلته لهم، كما يخير فيه أيضا الإمام بين القتل والاسترقاق والمن والفداء[6].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والخلاصة، أن الأصل في التجسس على عورات المسلمين التحريم سواء كانت الوسيلة في تحقيق ذلك تقليدية أو إلكترونية، بدليل قوله تعالى: ﴿ يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجْتَنِبُواْ كَثِيرًا مِّنَ ٱلظَّنِّ إِنَّ بَعْضَ ٱلظَّنِّ إِثْمٌ وَلَا تَجَسَّسُواْ وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَٱتَّقُواْ ٱللَّهَ إِنَّ ٱللَّهَ تَوَّابٌ رَّحِيمٌ ﴾[1]، وهو نهي موجه إلى آحاد المسلمين وجماعاتهم بمعنى: ولا تبحثوا عن عورات المسلمين وعيوبهم، وتستكشفوا عما ستر الله تعالى، كما نهت السنة النبوية الشريفة عن التجسس صراحة في قوله ﷺ : (إياكم والظن فإن الظن أكذب الحديث، ولا تحسسوا، ولا تجسسوا، ولا تناجشوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا، وكونوا عباد الله إخوانا)[2]، فيعاقب الذين يتجسسون على عورات الناس أو على معلوماتهم عن طريق أي وسيلة كانت بعقوبات تعزيرية تتراوح بين القتل والضرب والتنكيل والحبس وغيرها مما يقدره الحاكم وذلك بحسب الضرر الحاصل نتيجة جريمة التجسس، أما الحالات التي يجوز فيها التجسس فهي من صلاحيات ولي الأمر وحده ـــالدولة ـــ الذي يخول من يراه كفء في هذه المهمة بغرض حفظ المصالح العامة.

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثاني:
جريمة غسيل الأموال عن طريق الانترنت

ظاهرة غسيل الأموال هي واحدة من الأفعال المرتبطة بالجريمة المنظمة لاسيما جرائم الإرهاب، وتهريب الأسلحة، والمخدرات، والقمار، والسرقة، والفساد المالي وغيرها. وهي عملية تقوم على تهريب الأموال خارج حدود سريان القوانين المناهضة للفساد المالي، ثم تحاول العودة بها مرة أخرى بصفة شرعية ومعترف بها من قبل نفس القوانين المناهضة التي كانت تجرمها داخل الحدود الإقليمية التي تسري عليها هذه القوانين[1].

وكنتيجة للتقدم المذهل الذي بلغته التكنولوجيا وظهور التجارة الإلكترونية وما تتطلبه من وسائل دفع إلكترونية، استغل غاسلو الأموال من هذه المزايا وتمكنوا خلالها من الاتصال المباشر بأسواق المال العالمية دون عناء أو مشقة مستغلين في ذلك الخدمات العالمية لبنوك الانترنت والمراكز المصرفية والتحويلات الإلكترونية لإخفاء طابع الأموال ومصادرها الحقيقية.

ومثال ذلك ما تتيحه البنوك الإلكترونية من نقل أو تحويل كميات ضخمة من الأموال بسرعة وأمان وفي محيط يتميز بالسرية الشاملة، كما لا تخضع هذه البنوك لأية لوائح أو قوانين رقابية ولا تشكل لديها الحدود الوطنية عائـــقا أمام إجراء أي حجم من المعاملات المالية مع عدم إمكانية تعقبها، الأمر الذي سمح لمجرمي تبييض الأموال القيام من خلالها بمرحلتي التمويه المالي[2] ثم إدماجه[3] حيث يتمكنـــوا من تحويـــل أرصدتهم عدة مرات يوميا في أكثر من بنك عبر العالم، وبالتالي يصعب

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

تعقبهم أو كشف أمرهم.

المطلب الأول: مفهوم غسيل الأموال

الفرع الأول: التعريف اللغوي لغسيل الأموال

اقتصرت المعاجم اللغوية العربية على الإشارة إلى معنى الغسيل بصفة عامة، وهو إزالة الوسخ على الشيء أو التطهير من الإثم[1]، وغسل الشيء لغة، نظفه بالماء والاسم الغسل بالكسر ما يغسل به الرأس، قال الأخفش: ومنه الغسلين وهو ما انغسل من لحوم أهل النار ودمائهم، وزيد فيه الياء والنون، قال تعالى:﴿ وَلَا طَعَامٌ إِلَّا مِنْ غِسْلِينٍ ۝ لَّا يَأْكُلُهُۥٓ إِلَّا ٱلْخَٰطِـُٔونَ ﴾ [2].

واغتسل بالماء، والغسول الماء الذي يغتسل به وكذا المغتسل، ومنه قوله تعالى:﴿ هَٰذَا مُغْتَسَلٌۢ بَارِدٌ وَشَرَابٌ ﴾ [3]، والمغتسل أيضا الذي يغتسل فيه. والمغسل بفتح السين وكسرها مغسل الموتى والجمع المغاسل، والغسالة ما غسلت به الشيء، وشيء غسيل ومغسول.[4]

و المال في اللغة؛ كل ما يقتنى ويحوزه الإنسان بالفعل سواء أكان عينا أم منفعة، كذهب أو فضة أو حيوان أو نبات أو منافع الشيء كالركوب والملبس والسكنى، أما ما لا يحوزه الإنسان فلا يسمى مالا في اللغة كالطير في الهواء والسمك في الماء والمعادن في باطن الأرض، ويقال رجل مال أي كثير المال، وتمول الرجل، صار ذا مال، وموله غيره تمويلا [5].

الفرع الثاني: مفهوم غسيل الأموال في الاصطلاح الفقهي

غسيل الأموال هو من المصطلحات الحديثة نسبيا باعتبار حداثة الظاهرة، ولذلك لم تتطرق إليه كتب الفقه على سبيل الخصوص، إلا أن القرآن الكريم استوعب مفهوم غسيل الأموال من حيث التسمية والمضمون والمحتوى كما هو الشأن في اللغة العربية حيث قال عز وجل:﴿ وَلَا طَعَامٌ إِلَّا مِنْ غِسْلِينٍ ۝ لَّا يَأْكُلُهُۥٓ إِلَّا ٱلْخَٰطِـُٔونَ ﴾ [6]، فالياء والنون زائدان كما تبين في اللغة، وهذا يعني أن الحرام

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وغسيله لا يحقق الكفاية الاقتصادية ولا الثراء وإنما يحقق العقوبة والعذاب والندامة والزوال[1].

كما استوعبت هذا المفهوم مصادر الفقه الإسلامي وأشارت إليه في كتاب الغصب، حيث جاء في كتاب الهداية لابن جزي: " فإن غصب مسلم خمرا فخللها أو جلد ميتة فدبغه: فلصاحب الخمر أن يأخذ الخل بغير شيء .." والتخليل تطهير له بمنزلة غسل الثوب النجس فيبقى على ملكه؛ إذ لا تثبت المالية به"[2]، وهو ما يدل على استيعاب الفقه الإسلامي بأحكامه مسألة غسيل الأموال وذلك بالنظر إلى حرصه على وجوب تحقيق العدل والتوازن في اقتصاديات العقد، وأن يتم الحصول على المال بالطرق المشروعة وأن ينفق وينمى بالطرق المشروعة أيضا[3].

ويقول ابن رشد: " والأشياء الموجودة بأيدي الناس تنقسم إلى قسمين، أحدهما: ما لا يصح ملكه، والثاني: ما يصح، فأما ما لا يصح ملكه: لا يجوز بيعه بإجماع كالحر والخمر والخنزير والقرد والدم والميتة وما أشبه ذلك"[4]، ويقصد بذلك بيع الإنسان الحر أو ما يعرف الآن بالاتجار بالبشر وأعضاء جسم الإنسان، وكذلك بيع الخمر والمسكرات والمخدرات والمحرمات بجميع أنواعها وأشكالها، وقرر أن ما لا يجوز ملكه لا يجوز بيعه، وهو نص صريح في تحريم وتجريم غسيل الأموال؛ وبذلك يكون الفقهاء قد حرموا هذه الجريمة قبل صدور تجريمها في القوانين الوضعية.

الفرع الثالث: مفهوم غسيل الأموال في الاصطلاح الوضعي

اختلفت التشريعات وأراء المشرعين القانونيين في تحديد مفهوم جريمة غسيل الأموال بين مضيق وموسع؛ فجاء في التعريف الضيق أن غسيل الأموال يطلق على إخفاء أو تمويه المصدر غير المشروع للأموال المنقولة أو الموارد الناتجة عن جرائم المخدرات والمؤثرات العقلية، ويقصد بذلك إيجاد تبرير أو غطاء كاذب لمصدر الأموال الناتجة بصورة مباشرة أو غير مباشرة عن المتاجرة بالمخدرات. ويعاب على هذا التعريف حصره لمصادر غسيل الأموال في المتاجرة بالمخدرات وإغفاله عن الكثير من الأنشطة التي لا تقل خطورة عن جرائم المخدرات كالسرقة وتجارة السلاح وغيرها، وهو ما أخذت

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

به بعض القوانين كمشروع القانـــــون اللبناني في المادة "749" ، والتوصية الصادرة عن مجلس اتحاد المجموعة الأوروبية في 10 جوان 1991م المستلهمة من اتفاقية فيينا لعام 1988م[1].

وجاء في تعريف موسع؛ أن غسيل الأموال يطلق على كل عمل يهدف إلى إخفاء طبيعة أو مصدر الأموال الناتجة عن النشاطات الجرمية. ومن التشريعات التي اعتمدت هذا التعريف القانون الأمريكي عام 1986م، ومجموعة العمل المالي في التعاون لمكافحة تبييض الأموال التابعة لمنظمة التعاون والتنمية الاقتصادية في الأمم المتحدة، وهي تشمل الولايات المتحدة والمجموعة الأوروبية ومجلس التعاون الخليجي التي يطلق عليها مجموعة GAFI [2].

وجاء في القانون الجزائري رقم 05 ــ 01 المؤرخ في 27 ذو الحجة عام 1425 هــ الموافق لــ 06 فيفري 2005م، المتعلق بتبييض الأموال وتمويل الإرهاب ومكافحتهما في مادته الثانية ما يلي:

يعتبر تبييضا للأموال:

أ ــ تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تحصلت منها هذه الممتلكات، على الإفلات من الآثار القانونية لأفعاله.

ب ــ إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل أنها عائدات إجرامية.

ج ــ اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية.

د ــ المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة أو التواطؤ أو التآمر على ارتكابها أو محاولة ارتكابها والمساعدة أو التحريض على ذلك وتسهيله وإسداء المشورة بشأنه.

وبناء على هذه التعريفات وما اطلعت عليه يمكن استخلاص أن مصادر جريمة غسيل الأموال تتعدد بتعدد الأفعال غير المشروعة التي من أبرزها ما يلي[3]:

---

(1) الإحالات، في النسخة المطبوعة.

(2) الإحالات، في النسخة المطبوعة.

...../...

ـــ أنشطة الاتجار في السلع أو الخدمات غير المشروعة في الشريعة الإسلامية، وفي القوانين أو التشريعات الدولية، كالمتاجرة في المخدرات بأنواعها، وأنشطة البغاء والدعارة، أو شبكات الاتجار بالبشر.

ـــ أنشطة التهريب عبر الحدود للسلع والمنتجات المحلية أو المستوردة دون دفع الرسوم أو الضرائب الجمركية المقررة، كتـــهريب السلع من المناطق الحرة وتـــهريب السلع المعمرة والأسلحة وغيرها.

ـــ أنشطة السوق السوداء التي يتحقق منها مداخيل طائلة للمتعاملين فيها وعلى رأسها الاتجار في العملات الأجنبية.

ـــ أنشطة الرشوة والفساد الإداري والتربح من الوظائف العامة من خلال الحصول على مداخيل غير مشروعة مقابل التراخيص أو الموافقات الحكومية.

ـــ المداخيل الناتجة عن التهرب الضريبي من خلال التلاعب في الحسابات أو إخفاء مصادر الدخل وعدم سداد الضرائب المستحقة على النشاط إلى خزانة الدولة أو تحويل الأموال إلى خارج البلاد بإيداعها في البنوك الأجنبية.

ـــ العمولات التي يحصل عليها بعض الأفراد مقابل عقد صفقات الأسلحة والسلع الرأسمالية أو الاستثمارية أو الحصول على التكنولوجيا المتقدمة أو أية صفقات تجارية كبيرة.

ـــ المداخيل الناتجة عن الأنشطة السياسية غير المشروعة كأنشطة الجوسسة الدولية، والمداخيل الناتجة عن السرقات أو الاختلاسات من الأموال العامة.

ـــ الاقتراض من البنوك المحلية بدون ضمانات كافية وتحويلها إلى الخارج وعدم سداد المستحقات للبنوك المحلية، والهروب العمدي للأشخاص المقترضين مع أموالهم خارج البلاد لفترات إلى أن تسقط عنهم أحكام الجرائم بالتقادم.

ـــ جمع أموال المودعين وتهريبها إلى الخارج وإيداعها في البنوك الأجنبية دون توفير ضمانات كافية لأصحاب الأموال، مع قيام الأشخاص الذين يجمعون هذه الأموال بتحويلها إلى عقارات أو محلات تجارية أو غيرها ثم بيعها إلى ذويهم تمهيداً لعودة الأموال المسروقة إلى البلاد مرة أخرى في

(1) الإحالات في النسخة المطبوعة صورة مشروعة ظاهرا.
(2) الإحالات في النسخة المطبوعة.

.../.....

ـــ المداخيل الناتجة عن النصب والاحتيال المهربة إلى الخارج، كالاحتيال على طالبي العمل في الخارج لقاء مبالغ مقابل الحصول على شهادات أو جوازات مزورة.

ـــ المداخيل الناتجة عن الغش التجاري أو الاتجار في السلع الفاسدة أو تقليد الماركات العالمية أو المحلية ذات الجودة والشهرة الفائقة، أو تزوير النقود والكتب والمصنفات الفنية..

ـــ المداخيل الناتجة عن المضاربة غير المشروعة في الأوراق المالية والتي تعتمد على خداع المتعاملين في البورصات العالمية.

ولو تفحصنا هذه المصادر المالية وفق النظرة الشرعية لوجدناها ممنوعة في الدين الإسلامي، حيث ورد في معظمها أحكام صريحة تفيد التحريم كالمتاجرة بالخمور، والسرقة، والغش، والزنا، والقمار، والخيانة، والتجسس، والرشوة، كما نهت الشريعة الإسلامية عن كل ما يضر بالمجتمعات والأفراد مصداقا لقوله ﷺ: (لا ضرار ولا ضرار)[1]، وقد قال في ذلك ابن جزي: " إن أخذ أموال الناس بالباطل على عشرة أوجه، كلها حرام؛ الأول: الحرابة، والثاني: الغصب، والثالث: السرقة، والرابع: الاختلاس، والخامس: الخيانة، والسادس: الإذلال، والسابع: الفجور في الخصام، بإنكار الحق أو دعوى الباطل، والثامن: القمار، والتاسع: الرشوة، فلا يحل أخذها ولا إعطاؤها، والعاشر: الغش والخلابة في البيوع"[2].

وعلى هذا الأساس فإنني أضم رأيي إلى التعريف الموسع لجريمة غسيل الأموال لشموليته على جميع الجرائم المتعلقة بإخفاء طبيعة المال ومصادره.

المطلب الثاني: الآثار المترتبة على جريمة غسيل الأموال.

تعتبر جريمة غسيل الأموال أحد الظواهر التي تؤرق دول العالم بما فيها العالم الإسلامي، نظرا لآثارها السلبية التي تطول النواحي الاجتماعية والاقتصادية والسياسية للدولة وبيانها كما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أولا: الآثار الاجتماعية لجريمة غسيل الأموال.

من أبرز الآثار الاجتماعية التي تنتج عنها؛ الإخلال بالتركيبة الاجتماعية حيث تبرز ظاهرة الطبقية الاجتماعية وتعلو فيها طبقة الأغنياء بسبب تراكم الأموال غير المشروعة، فتزيد حدة التفاوت في توزيع الدخل، وتزيد معدلات الجرائم التي تغذيها الأموال غير المشروعة[1]، وهو ما ينعكس سلبا على المجتمع بتفشي الفساد وارتفاع عمليات السرقة والاختلاسات وانتشار أنواع الممارسات المحرمة والممنوعة كنوادي القمار والملاهي مما ينتج عنها تفشي الجريمة المنظمة داخل المجتمع[2].

كما يؤدي تسرب الأموال غير المشروعة بالمجتمع إلى انقلاب ميزان البناء الاجتماعي وذلك من خلال صعود المجرمين القائمين على عملية غسل الأموال إلى هرم المجتمع، في الوقت الذي يتراجع فيه مركز المكافحين إلى أسفل القاعدة، هذا إن لم تتضافر جهود المجتمع عامة في المكافحة[3].

ثانيا: الآثار الاقتصادية لجريمة غسيل الأموال

يعد الجانب الاقتصادي الأكثر تضررا من ظاهرة غسيل الأموال كونه المستهدف الأول الذي تنشأ في وسطه هذه الظاهرة، وذلك بسبب الاقتصاد الخفي الذي تنضوي تحته الأنشطة الغير مشروعة، ويمكن تلخيص أهم الآثار الناتجة عن ذلك كما يلي:

ـــ إن عدم مراعاة اعتبارات الربحية الذي تعتمده عمليات غسيل الأموال يؤثر سلبا على الاستثمار الدولي والمحلي لأن المنافسة تكون غير متكافئة بين المستثمر المحلي والأجنبي وهو ما يؤثر على حركة رؤوس الأموال وأسعار الصرف ومعدلات الفائدة، والذي بدوره يؤدي إلى الإخلال في مصداقية السياسات الاقتصادية وعدم استقرار أسواق المال دوليا[4].

ـــ كما أن عمليات التضليل في الإحصاءات الاقتصادية التي تعتمدها ظاهرة غسيل الأموال تظهر أن العوائد المحققة هي وليدة العمليات الإنتاجية والحقيقة عكس ذلك، وهو ما يؤدي إلى

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الإخلال بالقرارات الاقتصادية القومية نظرا لبنائها على أسس مظللة[1]، كمـــا يسبب ذلك خللا في وضع الخطط الناجحة لعملية التنمية الاقتصادية والاجتماعية[2].

ـــ ويؤدي تسرب الأموال المغسولة من الاقتصاد القومي للدول إلى زيادة العجز في ميزان المدفوعات وحدوث أزمة سيولة في النقد الأجنبي مما يهدد احتياطات الدولة لدى البنك المركزي من العملات المدخرة[3].

ـــ كما يؤدي تهريب رؤوس الأموال إلى الخارج الناتجة عن عملية غسيل الأموال إلى انخفاض معدلات الادخار المحلي الذي يؤثر بدوره في انخفاض المدخرات الموجهة للاستثمار فينعكس ذلك على تزايد معدلات البطالة التي تنشأ عن عدم وجود الفرص الاستثمارية المنتجة[4].

ـــ ويؤدي أيضا انتقال رؤوس الأموال إلى الخارج إلى انخفاض الإنتاج المحلي وانخفاض الدخل الخاضع للضريبة وهو ما يعطل تنفيذ السياسات المالية فينعكس سلبا على الميزانية العامة للبلد وعلى الأداء الاقتصادي والاجتماعي للموارد الحكومية[5]، وتؤدي هذه الظاهرة بدورها إلى زيادة السيولة المحلية بشكل لا يتوافق والزيادة الحاصلة في إنتاج السلع والخدمات مما ينتج عنه ضغوط تضخمية في الاقتصاديات المعنية[6].

ـــ كما تؤثر هذه الظاهرة في انهيار البورصات التي تستقبل الأموال الناتجة عن الجرائم الاقتصادية، وبذلك يتحول هدف شراء الأوراق المالية من البورصة لإتمام أحد مراحل تبييض الأموال بدل الاستثمار، ثم يتم بيع الأوراق المالية بشكل مفاجئ مما يؤدي إلى حدوث انخفاض حاد في أسعارها وهو ما يؤدي إلى انهيار البورصة[7].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ـــ ويؤدي غسيل الأموال بشكل عيني إلى ارتفاع حجم الواردات الأجنبية مما يسهم في اختلاف الحساب الجاري لميزان المدفوعات وزيادة عرض العملات الأجنبية على حساب العملات المحلية حيث تتجه هذه الأخيرة إلى الانخفاض خاصة في ظل الاتجاهات العالمية الراهنة التي تنادي بتطبيق سياسات اقتصادية أكثر انفتاحا على الاقتصاد العالمي[1].

ـــ كما يؤدي تنامي ظاهرة غسيل الأموال إلى زيادة نفقات الأمن لدى الدول المتضررة على حساب بقية القطاعات ولاسيما الاجتماعية منها، وذلك بهدف مكافحة التهرب الضريبي والجمركي وحماية المال العام والمرافق الأخرى، حيث تشير بعض البيانات أن نفقات الأمن تستحوذ على ما نسبته 27.4 بالمائة من إجمالي الإنفاق الجاري في الدول العربية لعام 2000م، كما تتكبد كبريات الشركات في الدول الصناعية تكاليف ضخمة تزيد على 20 في المائة من الأرباح لضمان مزيد من الحماية من الفساد والجريمة[2].

ثالثا: الآثار السياسية لجريمة غسيل الأموال

تساهم ظاهرة غسيل الأموال بشكل كبير في انتشار الرشوة والفساد الإداري وتفشي ما يسمى بالاقتصاد الأسود[3] الذي يعمل على إيصال فئة معينة من الأفراد إلى هرم الحكم وذلك عن طريق دعم حملاتهم الانتخابية بالأموال غير المشروعة، وينعكس ذلك على مجرمي غسيل الأموال بالحصانة والتأثير في القرارات المصيرية التي حتما ستعود بأضرار جسيمة على المجتمعات واقتصادياتها، فينتشر العنف والتطرف وهي بيئة تستغلها المنظمات الإجرامية ببيعها للأسلحة تشجيعا على تناحر أفراد المجتمع الواحد، وقد يؤدي ذلك إلى كسر الاستقرار الاجتماعي وتخريب الأنظمة الحاكمة في مختلف البلدان عن طريق نشر ظاهرة الصراع على السلطة السياسية[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المطلب الثالث: حكم جريمة غسيل الأموال عبر الانترنت

بناء على ما سبق، يتبين أن جريمة غسيل الأموال هي جريمة تبعية كونها تقوم على وقوع جريمة أخرى أصلية سابقة لها وهي المصدر غير المشروع للأموال المراد غسلها، لكنها تتنصل موضوعيا عن الجريمة الأولى مما يستلزم ملاحقة ومعاقبة من يقوم بغسيل الأموال ومن يشارك فيه، ومع ذلك تبقى الطبيعة المزدوجة للجريمة قائمة.

ولو تفحصنا مصادر وآثار جريمة غسيل الأموال بنظرة شرعية لتبين أنها تتنافى والضرورات التي أمر الشارع بحفظها؛ فعدم المبالاة بالحلال والحرام والتعدي على الحرمات من أجل كسب المال هو تعد على الدين، كما يعتبر تعد على النفس جريمة المتاجرة بالبشر وأعضائهم، والتجسس، ونشر الفتن، وترويج الأسلحة، وتخريب الأنظمة الحاكمة، كما تقوم جريمة غسيل الأموال على تجارة المخدرات والخمور، ونشر التطرف وكل ذلك يؤثر سلبا على العقل الذي أمر الشارع الحكيم بحفظه، و لم يسلم أيضا مقصد حفظ النسل من جريمة غسيل الأموال فالجرائم الجنسية تعد من أهم أنشطتها في جمع الموارد المالية، أما المقصد الشرعي الداعي لحفظ المال وعدم أكله بالباطل فإن الأصل في جريمة غسيل الأموال أنها تقوم على أساس أكل المال بالباطل ومحاولة تضليل الغير لاعتباره مالا حلالا، رغم أن ما يقوم على باطل يبقى باطلا، وكل ذلك محرم بنص القرآن والسنة والمعقول وبيانه كما يلي: [1]

أولا ــ أدلة التحريم من القرآن الكريم:

قال تعالى: ﴿ وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ وَتُدْلُواْ بِهَآ إِلَى ٱلْحُكَّامِ لِتَأْكُلُواْ فَرِيقًا مِّنْ أَمْوَٰلِ ٱلنَّاسِ بِٱلْإِثْمِ وَأَنتُمْ تَعْلَمُونَ ﴾[2].

فمنطوق الآية ومفهومها يشير إلى تحريم الحصول على أموال الناس بطرق غير مشروعة، كما تشير إلى الفساد المالي والوصول إلى الثراء غير المشروع، ويستلزم ذلك غسل الأموال المحرمة بالبداهة، حيث يقول القرطبي: " الخطاب بهذه الآية يتضمن جميع أمة محمد ﷺ والمعنى: لا يأكل بعضكم مال بعض بغير حق، فيدخل في هذا القمار والخداع، والغصوب، وجحد الحقوق، وما لا تطيب به نفسه مالكه، أو حرمته الشريعة وإن طابت به نفس مالكه، كمهـــر البغي وحلوان الكاهـــن وأثمان الخمور

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

والخنازير وغير ذلك... فهي دليل على أن الباطل في المعاملات لا يجوز..".[1]

وقال تعالى: ﴿ لَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٍ مِّنكُمْ ﴾[2].

ووجه الاستدلال؛ أن الآية أصل تشريعي عام تفيد تحريم أكل أموال الناس بطريق غير مشروع، وما يتبع ذلك من غسل للمال الحرام، كما أن الأصل في المعاملات المالية الرضا، والرضا منعدم في المعاملة التي تقوم على الحرام؛ لأن ما يقوم على الحرام يكون حراما وباطلا ابتداء. ويقول القرطبي في ذلك: " اعلم أن كل معاوضة تجارة على أي وجه كان العوض، إلا أن قوله " بالباطل" أخرج منها كل عوض لا يجوز شرعا من ربا أو جهالة أو تقدير عوض فاسد كالخمر والخنزير وغير ذلك"[3].

وقال تعالى: ﴿ إِنَّ ٱلَّذِينَ يَأْكُلُونَ أَمْوَٰلَ ٱلْيَتَٰمَىٰ ظُلْمًا إِنَّمَا يَأْكُلُونَ فِى بُطُونِهِمْ نَارًا ۖ وَسَيَصْلَوْنَ سَعِيرًا﴾[4]

ووجه الاستدلال من الآية الكريمة أنها أصل تشريعي عام يشمل بعموم جريمة غسل الأموال المحرمة.

وقال تعالى: ﴿ وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا ﴾[5]، ووجه الاستدلال؛ أن الآية الكريمة تشير إلى جريمة السرقة، وهي من مصادر المال الحرام الذي يغسل؛ ولهذا تشمل بعمومها وحكمها جريمة غسيل الأموال المحرمة.

وقال عز وجل: ﴿ فَمَنِ ٱعْتَدَىٰ عَلَيْكُمْ فَٱعْتَدُواْ عَلَيْهِ بِمِثْلِ مَا ٱعْتَدَىٰ عَلَيْكُمْ ﴾ [6].

فالمثلية في الآية تعني العدل، ومن يقوم بغسل المال الحرام يعتدي على الأمن الاقتصادي وما يلحقه من تبعات، ولهذا يجب وفق مقتضى الآية أن يكافح ويعاقب بنقيض قصده وفعله.

ثانيا ــ أدلة التحريم من السنة النبوية الشريفة:

قال النبي ﷺ في خطبة الوداع: (فإن دماءكم وأموالكم وأعراضكم عليكم حرام، كحرمة يومكم هذا، في بلدكم هذا في شهركم هذا، وأعادها مرارا، ثم رفع رأسه، فقال اللهم هل بلغت...)[7].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ووجه الاستدلال؛ أن الحديث يدل على عصمة مال المسلم وحرمة أخذه بطريق غير مشروع، وهو بعمومه يشمل جميع الجرائم المالية والاقتصادية ومنها جريمة غسيل الأموال.

وقال ﷺ : (لا يحل لأحدكم أن يأخذ متاع أخيه لاعبا ولا جادا، فإن أخذه فليرده عليه)[1].

فالحديث يدل صراحة على حرمة مال المسلم وعدم جواز أخذه بطريق غير مشروع ويتبع ذلك غسله، وإنما يجب أن يرد إلى صاحبه، وهذا دليل واضح على حرمة غسل الأموال المحرمة، فمن الواجب الشرعي أن ترد إلى أصحابها بقوة السلطان والقانون.

وقال النبي ﷺ: (يأتي على الناس زمان لا يبالي المرء بما أخذ المال بحلال أو حرام)[2].

ووجه الاستدلال؛ أن الحديث يدخل في باب التنبؤ العلمي وهو من أهداف العلم لأن العلم له أهداف ثلاثة؛ الفهم والتفسير، والضبط والتحكم، والتنبؤ، والحديث يشمل المال الحرام في زماننا ومن ذلك جريمة غسل الأموال المحرمة.

ثالثا ــ أدلة تحريم غسيل الأموال من المعقول:

يعتبر الاستقرار الاقتصادي من أهم أهداف السياسة الاقتصادية في الدولة الإسلامية ومن مقاصد الشريعة الواجب حفظها[3]، وكل ما يؤدي إلى الإخلال به أو زواله يكون باطلا عملا بقاعدة الذرائع، وقاعدة ما لم يتم الواجب إلا به فهو واجب، ولهذا أصبحت مكافحة جريمة غسيل الأموال عرفا عالميا للمحافظة على المال والاقتصاد، وحيثما تحققت المصلحة المعتبرة شرعا فذلك هو شرع الله ودينه.

كما تقوم جريمة غسيل الأموال على الحيل المحرمة التي يراد من خلالها إحلال الحرام، وقد عرّف الإمام الشاطبي الحيل الممنوعة بأنها: تقديم عمل ظاهر الجواز لإبطال حكم شرعي، وتحويله في الظاهر إلى حكم آخر، وعرّفها ابن القيم بأنها: إظهار أمر جائز ليتوصل به إلى أمر محرم يبطنه. وقد رتب العلماء على قاعدة سد الذرائع منع الحيل في الشريعة الإسلامية لأن العمل بالحيل هو خرق لقواعد الشريعة الإسلامية، وغسل الأموال حيلة محرمة مآلها خرق الأمن الاقتصادي للبلاد ولهذا يكون محرما

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

لأن حفظ المال من مقاصد الشريعة الإسلامية الثابتة[1].

وبناء على ذلك فإن غسيل الأموال هي جريمة محرمة شرعا، ويحرّم كل ما يفضي إليها من وسائل أو طرق سواء كانت تقليدية أو اعتمد في تحقيقها على وسائل التكنولوجيا الحديثة كشبكة الانترنت العالمية، وهو ما تدعمه القاعدة الفقهية المشهورة عند علماء الشريعة الإسلامية " **الوسائل لها أحكام المقاصد** " ، حيث أشار إليها القرافي بقوله: " **القاعدة أن الوسائل تتبع المقاصد في أحكامها، فوسيلة المحرم محرم، ووسيلة الواجب واجبة، وكذلك بقية الأحكام**"[2].

وقد قال ابن القيم عن هذه القاعدة: "لما كانت المقاصد لا يتوصل إليها إلا بأسباب وطرق تفضي إليها كانت طرقها وأسبابها تابعة لها معتبرة بها، فوسائل المحرمات والمعاصي في كراهتها والمنع منها بحسب إفضائها إلى غاياتها وارتباطاتها بها، ووسائل الطاعات والقربات في محبتها والإذن فيها بحسب إفضائها إلى غايتها؛ فوسيلة المقصود تابعة للمقصود، وكلاهما مقصود، لكنه مقصود قصد الغايات، وهي مقصودة قصد الوسائل؛ **فإذا حرم الله تعالى شيئا وله طرق ووسائل تفضي إليه فإنه يحرمها ويمنع منها** تحقيقا لتحريمه، وتثبيتا له، ومنعا أن يقرب حماه، ولو أباح الوسائل والذرائع المفضية إليه لكان ذلك نقضا للتحريم، وإغراء للنفوس به، وحكمته تعالى وعلمه يأبى ذلك كل الإباء، بل سياسة ملوك الدنيا تأبى ذلك..." [3].

فمؤدى القاعدة، أن الأفعال المتضمنة للمصالح والمفاسد في أنفسها ولها طرق تفضي إليها فإن تلك الطرق يختلف حكمها باختلاف حكم مقاصدها، فما يتوقف عليه الواجب واجب، وما لا يتم المسنون إلا به فهو مسنون، وما يتوقف الحرام عليه فهو حرام، ووسائل المكروه مكروهة، ووسائل المباح مباحة.

وعليه نخلص إلى أن غسيل الأموال عبر الانترنت هي جريمة اقتصادية محرّمة شرعا، تعاقب عليها الشريعة الإسلامية لمخالفتها للسياسة الاقتصادية التي هي جزء من السياسة الشرعية في الفقه الإسلامي، كما تستوجب عقوبات تعزيرية يحدد أمرها ومقدارها الحاكم المسلم أو من يقوم مقامه.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المبحث الثالث: جرائم الإرهاب الإلكتروني

يشير الإرهاب الإلكتروني إلى أوجه السلوك الإجرامي المقصودة والمستندة إلى دوافع عديدة ضد المعطيات الإلكترونية بأنواعها، ونظم وبرامج الكمبيوتر والاتصالات بهدف تحقيق أهداف إرهابية تنطوي على عنف يستهدف حياة الأفراد وسلامتهم، وإثارة الفوضى وعدم الاستقرار وإشاعة الخوف، وتعطيل الأداء الطبيعي لنظم السيطرة والرقابة الإلكترونية، وتعطيل عمل الأجهزة والهيئات الحكومية والمرافق الإستراتيجية في الدولة، وبوجه عام فإن الإرهاب الإلكتروني هو من الجرائم التي تستهدف المعطيات والنظم كهدف ومحل للجريمة، أو تستخدم الكمبيوتر والشبكات كوسيلة لارتكاب الجرائم التقليدية ضد الأشخاص والأموال، كما تستخدم الانترنت كبيئة للجريمة الإرهابية بما في ذلك نشر المواقع التي تمجد الإرهاب وتبرر عملياته وتموله، وتجنيد الإرهابيين، وجمع المعلومات التي تخدمهم، وتنفيذ عمليات إرهابية عن بعد وغيرها[1].

والإرهاب كمصطلح لم يرس على تعريف جامع يتفق عليه الناس، وسبب ذلك يعود إلى تأثر سائر التعريفات بخلفيات واضعيها وتصوراتهم عن الظاهرة، فما يعده البعض إرهابا يراه آخرون مقاومة ودفاعا عن الحقوق الشرعية المسلوبة، وبالرغم من تباين الآراء حول تعريف الإرهاب إلا أن هناك قاسم مشترك في أنه يقوم على العنف بقصد إثارة الخوف في نفوس الأفراد، وعلى هذا الأساس فإن الإرهاب الذي أبحثه هو ما يحصل به ما حرم الله تعالى من ترويع الآمنين، وتدمير مصالحهم ومقومات حياتهم، والاعتداء على أموالهم وحرياتهم وأعراضهم وكرامتهم بغيا وإفسادا في الأرض.

المطلب الأول: مدلول الإرهاب في اللغة والاصطلاح

الفرع الأول: تعريف الإرهاب في اللغة.

تتفق معاجـــم اللغة العربيـــة في مشتقات كلمة "رهب" بأنه الخوف والتخويف، والرعب أو

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الإرهاب بمعنى الإخافة والتخويف والفزع[1]. قال ابن منظور في اللسان: " رَهِبَ بالكسر يَرْهَبُ رَهبَةً ورُهْبًا بالضم، ورَهَبًا، بالتحريك أي خاف... وأرْهَبَهُ ورَهَّبَهُ واسْتَرْهَبَهُ: أخافه وأفزعه"[2].

وفي العادة تستخدم الرهبة في اللغة العربية للتعبير عن الخوف المقترن بالاحترام، وليس الخوف والرعب الناجم عن تهديد مادي، فيقال: رجل رهبوت، أي، رجل له مهابة واحترام[3]، وهذا المعنى الاصطلاحي أقره مجمع اللغة العربية حيث يفيد معنى الخوف المقترن بالاحترام والتوقير، وهو الرهبة والخوف والفزع، وليس "الإرهاب" الذي يعني الرعب والتخويف والترويع[4].

و لم يظهر لفظ "الإرهاب" "Terrorism" بالمعنى المعاصر إلا في المعاجم الحديثة، وهو مصدر من "أرهب"، بمعنى الأخذ بالتعسف والتهديد[5]، كما تعني كلمة "أرهب" محاولة نشر الذعر والفزع لأغراض سياسية[6]، ويعرّف الإرهاب بأنه: "رعب تحدثه أعمال العنف، مثل القتل وإلقاء المتفجرات، وذلك بهدف إقامة سلطة، أو تقويض سلطة أخرى"[7]، والإرهاب: بث الرعب الذي يثير الخوف والفزع[8].

الفرع الثاني: تعريف الإرهاب في الاصطلاح الفقهي

لم تذكر المدونات الفقهية القديمة أي تعريف لمصطلح "الإرهاب" و لم يفرد له باب بعينه وهو ما يقودنا إلى الإقرار بأن هذا المصطلح لم يحظ بتعريف علماء السلف، كما أن نصوص القرآن الكريم والسنة النبوية الشريفة تجاوزت صياغة أي تعريف منضبط له، وقد وردت مادة "رهب" ومشتقاتها في آيات القرآن الكريم وتعددت معانيها وفق السياقات التي جاءت في تلك الآيات المباركات لكن لا يشمل أي منها على تعريف لمصطلح جريمة "الإرهاب"، وذلك كما يلي:

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

أولا ــ مفهوم "الإرهاب" في القرآن الكريم:

لم يستعمل القرآن الكريم لفظ "الإرهاب" مطلقا، لكن احتوى على صيغ مختلفة الاشتقاق من نفس المادة اللغوية، حيث جاء لفظ "رهب" ومشتقاته في القرآن الكريم وكانت كلها تدور حول الرهبة والخوف والتحذير، أو الرهبنة والتعبد، ومن أمثلتها:

1 ــ في قوله تعالى: ﴿ وَأَوْفُواْ بِعَهْدِيٓ أُوفِ بِعَهْدِكُمْ وَإِيَّٰيَ فَٱرْهَبُونِ ﴾[1]، وكذلك قوله تعالى: ﴿ وَقَالَ ٱللَّهُ لَا تَتَّخِذُوٓاْ إِلَٰهَيْنِ ٱثْنَيْنِۖ إِنَّمَا هُوَ إِلَٰهٞ وَٰحِدٞۖ فَإِيَّٰيَ فَٱرْهَبُونِ ﴾[2].

ــ ﴿ وَلَمَّا سَكَتَ عَن مُّوسَى ٱلْغَضَبُ أَخَذَ ٱلْأَلْوَاحَۖ وَفِي نُسْخَتِهَا هُدًى وَرَحْمَةٞ لِّلَّذِينَ هُمْ لِرَبِّهِمْ يَرْهَبُونَ﴾[3].

ــ ﴿ لَأَنتُمْ أَشَدُّ رَهْبَةٗ فِي صُدُورِهِم مِّنَ ٱللَّهِۚ ذَٰلِكَ بِأَنَّهُمْ قَوْمٞ لَّا يَفْقَهُونَ ﴾[4].

ــ ﴿ إِنَّهُمْ كَانُواْ يُسَٰرِعُونَ فِي ٱلْخَيْرَٰتِ وَيَدْعُونَنَا رَغَبٗا وَرَهَبٗاۖ وَكَانُواْ لَنَا خَٰشِعِينَ ﴾[5].

فالرهبة في هذه الآيات تفيد معنى الخشية وتقوى الله سبحانه وتعالى والخوف منه[6]، حيث اشتملت على الذعر والفزع والخوف، ويقصد بذلك الخوف مع التعظيم لله سبحانه وتعالى، وما استعمال الرهبة في هذه الآيات إلا من باب العبادة والخوف من الله وخشيته[7].

2 ــ ﴿ قَالَ أَلْقُواْۖ فَلَمَّآ أَلْقَوْاْ سَحَرُوٓاْ أَعْيُنَ ٱلنَّاسِ وَٱسْتَرْهَبُوهُمْ وَجَآءُو بِسِحْرٍ عَظِيمٖ﴾ [8]، وهو وصف لحالة الناس حينما رأوا أعمال سحرة فرعون، فأصابهم الخوف والرعب والفزع من هذه الأعمال[9].

3 ــ ﴿ وَأَعِدُّواْ لَهُم مَّا ٱسْتَطَعْتُم مِّن قُوَّةٖ وَمِن رِّبَاطِ ٱلْخَيْلِ تُرْهِبُونَ بِهِۦ عَدُوَّ ٱللَّهِ وَعَدُوَّكُمْ وَءَاخَرِينَ مِن

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

دُونِهِمْ لَا تَعْلَمُونَهُمُ ٱللَّهُ يَعْلَمُهُمْ ﴾ [1]، و"رهب" في الآية تعني: الرعب والخوف في القتال في المعارك، بمعنى إخافة العدو، وتشير الآية إلى بث الرعب في قلوب الأعداء، وهو الردع المعروف في موازين القوى العسكرية[2].

4 ــ وقد وردت أيضا مشتقات المادة "رهب" في مواضع مختلفة من القرآن الكريم بمعنى الرهبنة والتعبد كما في قوله تعالى:

ــ ﴿وَجَعَلْنَا فِي قُلُوبِ ٱلَّذِينَ ٱتَّبَعُوهُ رَأْفَةً وَرَحْمَةً وَرَهْبَانِيَّةً ٱبْتَدَعُوهَا مَا كَتَبْنَاهَا عَلَيْهِمْ إِلَّا ٱبْتِغَآءَ رِضْوَٰنِ ٱللَّهِ فَمَا رَعَوْهَا حَقَّ رِعَايَتِهَا فَـَٔاتَيْنَا ٱلَّذِينَ ءَامَنُواْ مِنْهُمْ أَجْرَهُمْ وَكَثِيرٌ مِّنْهُمْ فَٰسِقُونَ ﴾[3]، والرهبانية العبادة[4].

ــ ﴿ إِنَّ كَثِيرًا مِّنَ ٱلْأَحْبَارِ وَٱلرُّهْبَانِ لَيَأْكُلُونَ أَمْوَٰلَ ٱلنَّاسِ بِٱلْبَٰطِلِ وَيَصُدُّونَ عَن سَبِيلِ ٱللَّهِ ﴾[5]، وقال تعالى: ﴿ ٱتَّخَذُوٓاْ أَحْبَارَهُمْ وَرُهْبَٰنَهُمْ أَرْبَابًا مِّن دُونِ ٱللَّهِ ﴾[6]، والرهبان هنا من "رهِب"، ومعناه الخوف والخشية، و"راهب" الخائف من الله المتعبد في صومعته، وجمعه "رهبان".

ولقد تفحصت العديد من كتب التفاسير وما لاحظته أن المفسرين لم يخرجوا في بيان معنى "رهب" وما اشتق منها عما أورده علماء اللغة والبيان، فيقول ابن كثير في تفسيره: (وإياي فارهبون) أي فاخشوني، من الترهيب، والرهبة من أجل الرجوع إلى الحق، والاتعاظ بما عسى أن يترل بهم من العقاب[7]، كما فسر قوله تعالى:﴿ وَقَالَ ٱللَّهُ لَا تَتَّخِذُوٓاْ إِلَٰهَيْنِ ٱثْنَيْنِ إِنَّمَا هُوَ إِلَٰهٌ وَٰحِدٌ فَإِيَّٰىَ فَٱرْهَبُونِ ﴾[8]، أي ارهبوا أن تشركوا بي شيئا وأخلصوا الطاعة[9]، وجاء في تفسيره قوله تعالى:﴿ وَيَدْعُونَنَا رَغَبًا وَرَهَبًا﴾[10]، قال: رغبا فيما عندنا، ورهبة مما عندنا، خائفين خاشعين، الخشوع هو الخوف المستمر، خاشعين أي متواضعين[11].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

.../.....

ولم يخرج الشوكاني أيضا عما جاء به ابن كثير عن بيان "الرهبة" في الآيات القرآنية السابقة، ومن ذلك تفسيره لقوله الله عز وجل: ﴿فَإِيَّىَ فَٱرۡهَبُونِ﴾ قال: "فاخشون أن أنزل عليكم ما أنزلته بمن قبلكم من العذاب والعقاب، بما أخلفوا ما عاهدوا الله عليه وعصوا أوامره، وأكثروا في الأرض الفساد"[1].

وجاء في تفسير ابن كثير لقوله تعالى:﴿ تُرۡهِبُونَ بِهِۦ عَدُوَّ ٱللَّهِ وَعَدُوَّكُمۡ ﴾[2]، ترهبون: أي تخوِفون[3]، وهو ما جاء به كذلك ابن العربي حيث يقول: يعني تخيفون بذلك أعداء الله وأعداءكم من اليهود وقريش وكفار العرب[4]، وهو ما جاء به أيضا القرطبي في الجامع لأحكام القرآن[5]، فالإرهاب المقصود في الآية إنما هو تخويف العدو إذا كان بينه وبينهم حالة حرب معلنة وواضحة وهي حالة الصراع بين الحق والباطل، وليس المراد في الآية إرهاب الآمنين أو تخويفهم.

ثانيا ــ مفهوم الإرهاب في السنة النبوية الشريفة:

لم يستعمل في السنة النبوية الشريفة لفظ "الإرهاب" مطلقا، إنما احتوت الأحاديث الشريفة على كلمة "رهب" ومشتقاتها، وهي تحمل المعنى نفسه الذي جاء به القرآن الكريم ويتوافق مع ما جاءت به معاجم اللغة العربية القديمة كالخوف ونحوها، ومثال ذلك ما روي عن البراء بن عازب أن النبي ﷺ أوصى رجلا فقال: (إذا أردت مضجعك فقل: اللهم أسلمت نفسي إليك، وفوضت أمري إليك، ووجهت وجهي إليك، وألجأت ظهري إليك رغبة **ورهبة** إليك، لا ملجأ إلا إليك، آمنت بكتابك الذي أنزلت وبنبيك الذي أرسلت، فإن مت مت على الفطرة)[6]، والرهبة في الحديث: الخوف والفزع، حيث جمع بين الرغبة والرهبة، ثم أعمل الرغبة وحددها[7].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وجاء في حديث (لا **رهبانية** في الإسلام)[1]، وهي من رهبنة النصارى، وأصل الرهبانية من الرهبة، وهي: الخوف والفزع، فقد كانوا يترهبون بالتخلي من شواغل الدنيا ويتركون ملاذها، وكذلك الزهد فيها، والعزلة عن أهلها، وتعمد مشاقها، فنبذها النبي ﷺ ونهى المسلمين عنها[2].

ثالثا ــ مفهوم الإرهاب في الاصطلاح الفقهي المعاصر:

عرّف التشريع الإسلامي الجرائم على وجه الإجمال والتفصيل، وصنف أشد الأعمال جرما وأعظمها إثما، وهو ما تطرقت إليه القوانين والاتفاقيات الدولية المعاصرة على أنها أفعال إرهابية، ومن تلك الأعمال:

ــ القتل العمد عدوانا لمعصوم الدم، وحكمه التحريم، وعقوبته في الشريعة الإسلامية حد القتل، حيث قال تعالى:﴿ مِنْ أَجْلِ ذَٰلِكَ كَتَبْنَا عَلَىٰ بَنِيٓ إِسْرَٰٓءِيلَ أَنَّهُۥ مَن قَتَلَ نَفْسًۢا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِى ٱلْأَرْضِ فَكَأَنَّمَا قَتَلَ ٱلنَّاسَ جَمِيعًا ﴾[3]، وقال تعالى: ﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ كُتِبَ عَلَيْكُمُ ٱلْقِصَاصُ فِى ٱلْقَتْلَىٰ ﴾[4]، وقال عز وجل:﴿ وَمَن يَقْتُلْ مُؤْمِنًا مُّتَعَمِّدًا فَجَزَآؤُهُۥ جَهَنَّمُ خَٰلِدًا فِيهَا ﴾[5]، وقال سبحانه وتعالى: ﴿ وَلَا تَقْتُلُواْ ٱلنَّفْسَ ٱلَّتِى حَرَّمَ ٱللَّهُ إِلَّا بِٱلْحَقِّ ﴾[6].

ــ الإفساد في الأرض، كقطع الطريق وترويع الآمنين ونحوها، وهو من كبائر الذنوب، وجزاؤه إما القتل أو الصلب، أو تقطيع الأيدي والأرجل من خلال، أو السجن، إضافة إلى عذاب الآخرة، كما في قوله تعالى: ﴿ إِنَّمَا جَزَٰٓؤُاْ ٱلَّذِينَ يُحَارِبُونَ ٱللَّهَ وَرَسُولَهُۥ وَيَسْعَوْنَ فِى ٱلْأَرْضِ فَسَادًا أَن يُقَتَّلُوٓاْ أَوْ يُصَلَّبُوٓاْ أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُم مِّنْ خِلَٰفٍ أَوْ يُنفَوْاْ مِنَ ٱلْأَرْضِ ۚ ذَٰلِكَ لَهُمْ خِزْىٌ فِى ٱلدُّنْيَا ۖ وَلَهُمْ فِى ٱلْءَاخِرَةِ عَذَابٌ عَظِيمٌ﴾[7].

---

(1) الإحالات في النسخة المصوغة.

(2) الإحالات في النسخة المطبوعة.

...../...

وهكذا نجد أن الإسلام قد أعطى مفهوما واضحا للإرهاب على اعتبار تعريفه وفق وقائع وأفعال معينة[1].

وقد تطرق الفقه الإسلامي المعاصر لظاهرة الإرهاب وذلك من خلال قرارات المجامع الفقهية الإسلامية وفتاوى العلماء والفقهاء المعاصرين والكتاب الإسلاميين، من بينها ما يلي:

جاء مفهوم الإرهاب عن المجمع الفقهي الإسلامي في دورته السادسة عشرة عام 1422هـ كما يلي: " هو العدوان، الذي يمارسه أفراد أو جماعات أو دول، **بغيا** على الإنسان في (دينه ودمه وعقله وماله وعرضه)، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق، وما يتصل بصورة **الحرابة** وإخافة السبيل وقطع الطريق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة، أو بأحد المرافق والأملاك العامة أو الخاصة، أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر، فكل هذا من صور الفساد في الأرض، التي نهى الله سبحانه وتعالى المسلمين عنها"[2].

الفرع الثالث ــ مفهوم الإرهاب في اللوائح والاتفاقات الوضعية:

أجمعت القوانين الوضعية على تجريم ظاهرة الإرهاب لما ينتج عنه من آثار سلبية شديدة الخطورة على الأمن القومي، لكنها اختلفت في تحديد معنى واضحا للظاهرة وهذا راجع إلى المعايير التي تم اعتمادها في تعريف الظاهرة والتي تختلف من دولة إلى أخرى، ومن ذلك ما نصت عليه الفقرة الثانية من المادة الأولى في اتفاقية جنيف المبرمة في 16 نوفمبر 1937م لتجريم الإرهاب، والخاصة بتعريف الإرهاب على أنه: يمثل أفعالا إجرامية موجهة ضد الدولة، التي يكون هدفها أو طبيعتها، إشاعة الفزع أو الخوف في نفوس كافة الشعوب، وقد فصلت تلك الأفعال الإرهابية في المادة الثانية من نفس الاتفاقية كما يلي:

1 ــ كل فعل عمدي، يتسبب في موت، أو إحداث إصابة جسيمة، أو فقدان حرية أي من:

أ ــ رؤساء الدول، والقائمين بأعمالهم، أو ورثتهم أو خلفائهم.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ب ـــ زوجات وأزواج أي من الفئات السابقة.

ج ـــ الأشخاص القائمين بمسؤوليات عامة، أو من ذوي المناصب العامة، إذا وجهت هذه الأفعال إليهم بصفاتهم هذه.

2 ـــ التخريب المتعمد، أو إتلاف الممتلكات العامة، أو الممتلكات المخصصة لأغراض عامة، والمتعلقة أو الخاضعة لسلطات دولة أخرى من الدول المتعاقدة.

3 ـــ كل فعل عمدي يعرض حياة العامة للخطر.

4 ـــ الشروع في ارتكاب فعل من الأفعال السابقة، والمشار إليها في هذه المادة.

5 ـــ تصنيع، أو الحصول أو حيازة، أو إمداد الأسلحة والمؤن والمتفجرات، أو أي مواد ضارة بقصد ارتكاب أي من الأفعال السابقة، في أي دولة من الدول أيا كانت، مما يدخل في نطاق الأفعال السابقة الإشارة إليها في الاتفاقية[1].

كما عرّف الإرهاب في المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب التي صدرت بالقاهرة عام 1998م، بأنه: "كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إفشاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر"[2].

الفرع الرابع ـــ مفهوم الإرهاب الإلكتروني:

إن إطلاعي على التعريفات المتعلقة بالإرهاب الإلكتروني جعلتني ألاحظ تقاربها في المفاهيم وذلك من جهة الترويع والفساد والتخريب باستعمال وسائل التكنولوجيا الحديثة، ومن بين هذه التعريفات ما يلي:

يعرّف الإرهاب الإلكتروني على أنه: رعب تنشره دولة أو جماعة أو أفراد، سرية كانت أو علنية عن طريق استخدام الوسائل الإلكترونية بالقتل أو التخريب أو الإفساد بأي صورة من صوره أو التهديد بشيء من ذلك ضد السلطة الشرعية[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

و يعرّف بأنه: العدوان أو التخويف أو التهديد حسيا كان أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض[1].

وعلى ضوء ذلك يمكن استنتاج تعريفا للإرهاب الإلكتروني؛ بأنه الترويع الحسيُّ أو المعنويُّ المقصود للآمن باستخدام الوسائل الإلكترونية الحديثة بغرض تحقيق أهداف تتنافى ومقاصد الدين الإسلامي.

فالإرهاب الإلكتروني يشمل كل ترهيب أو تخويف عن قصد يلحق بالضحية ضررا ماديا أو معنويا، سواء صدر من فرد أو جماعة أو دولة وذلك سعيا إلى تحقيق أهداف غير شرعية مطلقا كتضليل الناس عن الدين الإسلامي أو سفك الدماء وانتهاك الأعراض، وإتلاف الأموال وغير ذلك من ضروب الفساد في الأرض.

المطلب الثاني: حكم الإرهاب باعتبار علاقته بالحرابة

تعد جريمة الحرابة في الفقه الجنائي الإسلامي من أخطر الجرائم لما فيها من خروج على سلطان الدولة وترويع الناس والاعتداء على الأموال العامة والخاصة وعلى أرواح الناس[2]، وهو ما ينطبق على إحدى العناصر المميزة للعمل الإرهابي وما ينتج عنها من خوف وفزع ورعب، وعدم الطمأنينة[3]. كما تتحقق الحرابة بخروج فرد من الأفراد، أو بخروج جماعة من الجماعات، وقد أدرج كثير من أهل العلم في مفهوم الحرابة العصابات المختلفة كعصابات القتل وعصابة خطف الأطفال، وعصابة اللصوص التي تسطو على المساكن والبنوك والمتاجر، وعصابة خطف النساء للفجور بهن، وحتى العصابات التي تتلف المزروعات وتقتل المواشي والدواب على سبيل الإفساد[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

ولإثبات التقارب بين الحرابة وظاهرة الإرهاب لابد من الإشارة إلى معنى الحرابة في اللغة وفي الاصطلاح الفقهي.

الفرع الأول: التعريف اللغوي للحرابة

الحرابة في اللغة: المحاربة، على وزن مفاعلة من الحرب، وهي ضد السلم، والأصل في كلمة "الحرب" التعدي وسلب المال، والأصل كذلك في "المحاربة": الاعتداء والسلب وإزالة الأمن، وقد يكون ذلك بقتل وقتال، وقد يكون بدونهما، وهذا لا يتصل بالمعنى المعروف للحرب، لأن المحاربة مفاعلة، ولذلك سميت كذلك "الحرابة" للفرق بينها وبين الحرب[1].

والحرابة من الحرب، وحربه حرباً، إذا أخذ ماله وتركه بلا شيء، والمحروب: هو المسلوب والمنهوب، والمحارب: هو الغاصب الناهي، والمحارب اسم فاعل، مشتق من حارب، والحرب: نقيض السلم، بمعنى سلب الأموال، وهي بمعنى القتل، وتدل على وجه العموم بمعنى الغصب[2].

والأصل في الحرابة الاعتداء والسلب وإزالة الأمن، وذلك بالاقتتال أو بدونهما، وهو ما يتفق مع مفهوم الإرهاب وما يصدر منه من اعتداء على الآمنين، ومن أعمال تخريبية وعدم الاستقرار.

الفرع الثاني: التعريف الاصطلاحي للحرابة

الحرابة في الاصطلاح الفقهي هو إشهار السلاح وقطع السبيل خارج المصر أو داخله، واشترط الشافعية أن يكون ذلك من أهل الشوكة كالعصابات المسلحة للسلب والنهب، أو جماعات مقاومة السلطة ابتغاء الفتنة وابتغاء الفساد، حيث يقول الإمام الشافعي: " إنه إذا ضعف السلطان، ووجدت المغالبة في المصر أي الإقليم الخاضع للسلطان كانت محاربة"، بينما ذهب الإمام أبو حنيفة بأن المحاربة لا تكون إلا خارج المصر باعتبار أن قطع الطريق يثبت في الصحراء، لأن في المدن قد يتوفر فيها الغوث والحماية، فتزول شوكة المعتدين، في حين يرى بعض الحنابلة والشافعية أن الضرر أعظم في المصر، ويرى الإمام مالك: أن يكون الفعل على وجه يتعذر معه الغوث داخل العمران أو خارجه[3].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

كما يعتبر المحارب هو كل من كان دمه محقونا قبل الحرابة، وهو المسلم والذمي[1]، والمحارب هو المكابر المخيف لأهل الطريق المفسد في سبيل الأرض سواء بالسلاح أو بغيره ليلا أو نهارا، في مصر أو فلاة، وسواء فعل ذلك بجند أو غير جند، أي هو من حارب المارة، وأخاف السبيل، بقتل نفس، أو أخذ مال، أو انتهاك عرض[2].

ويتضح من خلال هذه التعريفات أن المحارب هو: " كل من خرج لإخافة السالكين في الطريق، أو لأخذ أموالهم أو قتلهم أو جرحهم، إذا كان بسلاح ليلا أو نهارا"[3]، كما أن الحرابة تقوم على عنصرين أساسيين وهو ما تقوم عليه أيضا الأعمال الإرهابية[4]:

1 ــ المجاهرة اعتمادا على الشوكة، وهي أحد صفات العمل الإرهابي في غالبيته، وذلك يؤدي إلى امتناع الناس من استعمال الطريق بدافع الخوف والفزع حفاظا على أموالهم وأرواحهم، كما لا يمنع ذلك من اختفاء المحاربين عن أعين الحاكم أو من يمثله، إلا أن أعمالهم تتم مجاهرة وهو ما يميز الحرابة عن جريمة السرقة.

2 ــ في الغالب يكون القصد من وراء العمل الإجرامي، هو تحقيق مصلحة مادية بالحصول على المال ولو أدى ذلك إلى القتل مما ينتج عنه إرهاب الآمنين وترويعهم، ويعتبر هذا العمل إرهابيا سواء صحب إثارة الخوف والرعب أخذ المال أو قتل، أو لم يحصل شيء من ذلك، لأن إخافة السبيل تتحقق بها جريمة الحرابة عند جمهور الفقهاء حتى لو لم يتحقق أخذ مال أو قتل نفس.

وبهذا يتضح مدى التقارب بين مفهوم الحرابة ومفهوم الإرهاب والأعمال الإرهابية الحديثة، وهو ما جعل الكثير من الفقهاء المعاصرين يدرجون عقوبة الحرابة بالإرهابيين، والتي يعود أصلها إلى قوله تعالى: ﴿ إِنَّمَا جَزَٰٓؤُاْ ٱلَّذِينَ يُحَارِبُونَ ٱللَّهَ وَرَسُولَهُۥ وَيَسۡعَوۡنَ فِي ٱلۡأَرۡضِ فَسَادًا أَن يُقَتَّلُوٓاْ أَوۡ يُصَلَّبُوٓاْ أَوۡ تُقَطَّعَ أَيۡدِيهِمۡ وَأَرۡجُلُهُم مِّنۡ خِلَٰفٍ أَوۡ يُنفَوۡاْ مِنَ ٱلۡأَرۡضِۚ ﴾[5].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وعقوبة الحرابة تختلف عند أبي حنيفة والشافعي وأحمد باختلاف الأفعال التي تصدر من المحارب كإخافة السبيل دون أخذ المال أو القتل، أو أخذ المال لا غير، أو أخذ المال والقتل معا، فلكل فعل من هذه الأفعال عقوبة خاصة باعتبار الآية. أما الإمام مالك فيرى أن القاضي مخير في تنزيل أحد العقوبات الواردة في الآية ماعدا القتل فيعاقب الجاني إما بالقتل أو القتل والصلب، بينما يخير القاضي عند الظاهرية في تحديد العقوبة المناسبة أيا كانت الجريمة[1].

المطلب الثالث: حكم الإرهاب باعتبار علاقته بالبغي

من مقاصد الشريعة الإسلامية أن تتسم الدولة الإسلامية بالقوة والوحدة، يحكمها إمام عادل يُطبق فيها شريعة الإسلام ويسودها العدل والاستقرار على جميع الأصعدة السياسية والاجتماعية والاقتصادية..، وهو ما يتنافى وجريمة البغي لما يصدر منها من أفعال تخل بالنظام العام؛ فتشيع الفتن وما يرافقها من سفك للدماء واستباحة الحقوق وتخريب وتبديد ثروات الأمة، وما يلحق ذلك من إضرار بوحدة الأمة السياسية، ولذلك يعتبر البغي اعتداء على حقوق الله في حفظ أمن الجماعة المسلمة وضمان استقرارها، واعتداءً على حقوق الناس.

ولقد اعتبر العديد من الباحثين الإسلاميين أن جريمة البغي في الشريعة الإسلامية هي مرادف لمفهوم الإرهاب الحديث، باعتبار أن العنصر الجوهري المميز للعمل الإرهابي هو الهدف السياسي، ولذلك فإن البغي هو إحدى صوره[2]، كما هو الشأن فيما يخص جريمة الحرابة[3]، بينما يرى اتجاه آخر أن جريمة البغي هي نوعا من التعصب لرأي معين، نتيجة الاختلاف في فهم الأحكام الشرعية الأمر الذي جعل بعض الفقهاء يصنفون البغي إلى البغي بحق، والبغي بغير حق وهو البغي الباطل الذي يعد جريمة تستوجب صدّها[4].

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الأول: التعريف اللغوي للبغي

البغي في اللغة طلب الشيء فيقال بغيت كذا إذا طلبته، ومن ذلك قوله تعالى: ﴿ قَالَ ذَٰلِكَ مَا كُنَّا نَبْغِۚ ﴾[1]، ثم اشتهر البغي في العرف في طلب ما لا يحل من الجور والظلم، وإن كانت اللغة لا تمنع من أن يكون البغي بحق ومن ذلك قوله تعالى: ﴿ قُلْ إِنَّمَا حَرَّمَ رَبِّيَ ٱلْفَوَٰحِشَ مَا ظَهَرَ مِنْهَا وَمَا بَطَنَ وَٱلْإِثْمَ وَٱلْبَغْيَ بِغَيْرِ ٱلْحَقِّ ﴾[2].

والبغي هو مجاوزة الحد، يقال بغى بغيًا: تجاوز الحد واعتدى، والبغي مجاوزة الحد، والظلم، والخروج على النظام، والتعدي، والعدول عن الحق، والاستطالة على الناس، والفساد[3]، وأصل ذلك قوله تعالى:﴿ وَإِن طَآئِفَتَانِ مِنَ ٱلْمُؤْمِنِينَ ٱقْتَتَلُواْ فَأَصْلِحُواْ بَيْنَهُمَاۖ فَإِنۢ بَغَتْ إِحْدَىٰهُمَا عَلَى ٱلْأُخْرَىٰ فَقَٰتِلُواْ ٱلَّتِي تَبْغِي حَتَّىٰ تَفِيٓءَ إِلَىٰٓ أَمْرِ ٱللَّهِۚ ﴾[4]. وقد خص الفقهاء بالبغي الخروج على الإمام، إما بالامتناع عن أداء الواجب، وإما بعدم الانقياد والطاعة[5].

الفرع الثاني: تعريف البغي في الاصطلاح الفقهي.

يعرِّف البغي عند الحنفية بأنه: "الخروج عن طاعة إمام الحق بغير الحق"[6]، ويعرّفون البغاة بأنهم: "كل فئة لهم منعة، يتغلبون، ويجتمعون، ويقاتلون أهل العدل بتأويل"[7].

والبغاة عند المالكية: هم فرقة خالفت الإمام لمنع حق، أو لخلعه[8]، فالبغاة عندهم هم الذين يقاتلون على التأويل كالطوائف الضالة الذين يخرجون على الإمام أو يمتنعون من الدخول في طاعته أو يمنعون حقاً وجب عليهم كالزكاة ونحوها[9].

أما الشافعية فعرّفوا البغاة بأنهم: المخالفين للإمام الخارجين عن طاعته بترك الانقياد أو الامتناع عن أداء واجب، بشـــرط أن يكون لهم تأويل، يعتقد بسببه جواز الخروج، وأن تكون لهم شوكـــة،

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

فالبغاة هم طائفة من المسلمين خالفوا رأي الجماعة، وانفردوا بمذهب ابتدعوه[1].

وعرّف الحنابلة البغاة بأنهم: الظلمة، الخارجون عن طاعة الإمام، المعتدون عليه[2]، أو هم: البغاة الخارجون على الإمام بتأويل سائغ، ولهم شوكة"[3].

والملاحظ من تعريفات المذاهب لجريمة البغي، أنها تقوم على التأويل الذي يعتقدون أنه سائغ من وجهة نظرهم كقولهم بأن ولاية ولي الأمر غير شرعية، بالإضافة إلى تمتع البغاة بالقوة والمنعة واتخاذهم قائدا لهم يمثلهم، ولذلك لا تسري أحكام البغاة شرعا إلا على الخارجين على الإمام بتأويل[4].

فتحقق شرط " التأويل" لازم في جريمة البغي، على أن يكون الخروج موجها ضد السلطة السياسية للدولة، وهو ما يعبر عنه حديثا بالجريمة السياسية[5]، الأمر الذي يقودنا إلى القول بأن جريمة البغي بغير حق هي أقرب ما تكون إلى الإرهاب السياسي في المفهوم الحديث للإرهاب، لأن التقارب واضح بين الهدف السياسي للأعمال الإرهابية وبين التأويل الذي يشترطه الفقهاء في جريمة البغي[6]، وبذلك يكون مفهوم جريمة البغي بشروطها[7] التي اتفق عليها الفقهاء مفهوما دقيقا للإرهاب السياسي في الفقه الإسلامي.

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الفرع الثالث: حكم جريمة البغي وعقوبتها

يعد البغي من الجرائم المنهي عنها والمحرمة في الشريعة الإسلامية، حيث يقول عز وجل: ﴿إِنَّمَا ٱلسَّبِيلُ عَلَى ٱلَّذِينَ يَظْلِمُونَ ٱلنَّاسَ وَيَبْغُونَ فِى ٱلْأَرْضِ بِغَيْرِ ٱلْحَقِّ ۚ أُو۟لَٰٓئِكَ لَهُمْ عَذَابٌ أَلِيمٌ﴾[1]، وعقوبة البغي القتل، وأصل ذلك قوله تعالى:﴿ وَإِن طَآئِفَتَانِ مِنَ ٱلْمُؤْمِنِينَ ٱقْتَتَلُوا۟ فَأَصْلِحُوا۟ بَيْنَهُمَا ۖ فَإِنۢ بَغَتْ إِحْدَىٰهُمَا عَلَى ٱلْأُخْرَىٰ فَقَٰتِلُوا۟ ٱلَّتِى تَبْغِى حَتَّىٰ تَفِىٓءَ إِلَىٰٓ أَمْرِ ٱللَّهِ ۚ فَإِن فَآءَتْ فَأَصْلِحُوا۟ بَيْنَهُمَا بِٱلْعَدْلِ وَأَقْسِطُوٓا۟ ۖ إِنَّ ٱللَّهَ يُحِبُّ ٱلْمُقْسِطِينَ ﴾[2].

كما ورد تحريم البغي في العديد من الأحاديث النبوية الشريفة التي تذم البغي وتنهى المسلمين عن محاربة ولاة الأمر الشرعيين وتحث على طاعتهم ما لم يأمروا بمعصية أو منكر، كما تحث على التزام جماعة المسلمين وعدم التورط في الفتن وسفك الدماء المحرمة، أو الاعتداء على الأموال والأرواح دون مبرر شرعي، ومن هذه الأحاديث ما رواه مسلم عن أبي هريرة أن النبي ﷺ قال: (من خرج من الطاعة وفارق الجماعة فمات، مات ميتة جاهلية، ومن قاتل تحت راية عمية يغضب لعصبة أو يدعو إلى عصبة أو ينصر عصبة فقتل، فقِتلة جاهلية، ومن خرج على أمتي يضر برها وفاجرها ولا يتحاشى من مؤمنها ولا يفي لذي عهد عهده فليس مني ولست منه)[3].

وعن عَرْفَجَةَ رضي الله عنه، قال: سمعت رسول الله ﷺ يقول: (إنه ستكون هَنَاتٌ وهَنَاتٌ وهناتٌ[4]، فمن أراد أن يفرق أمر المسلمين وهم جميع فاضربوه بالسيفِ كائنًا من كان)[5]، وهو حكم صريح بقتال من خرج على الإمام، أو أراد تفريق كلمة المسلمين، حيث يُنهى عن ذلك فإن لم ينته قوتل، وإن لم يندفع شره إلا بقتله فقتله كان هدرًا.

وهي أدلة تبين أن أصل البغاة هم من المسلمين، فيخرجون عن وحدة حكم الإمام ويخالفون الجماعة وينفردون بمذهب ابتدعوه لتأويل سائغ في نظرهم، وفيهم منعة، ويحتاج في كفهم إلى جمع الجيش وقتالهم[6]، ولذلك فإن صفة البغي تنطبق على كل عمل إجرامي تتحقق فيه الأركان الأساسية

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الثلاثة وهي: الخروج عن الإمام، وأن يكون الخروج مغالبة أي باستعمال القوة، وأن يصحب الخروج القصد الجنائي، والقصد المطلوب توفره هو القصد الجنائي العام، أي قصد الخروج على الإمام مغالبة، فإذا كان الخارج لم يقصد من فعله الخروج على الإمام أو لم يقصد المغالبة فهو ليس باغيا[1]. أما إذا تحققت تلك الأركان يصبح القتال فرضا موجه على سبيل الوجوب إلى السلطات وإلى عامة المواطنين، وبناء على ذلك فإن الباغي مُهدر الدم والمال ولكن وفق شروط وضوابط شرعية محددة، ويبقى أجل إهدار دم البغاة قائما إلى أن ترجع الفئة الباغية إلى أمر الله تعالى، حينذاك يحل "الإصلاح والإقساط " ـــ كما ورد في الآية ـــ محل القتال، وما يتفرع عنه من إهدار للدم، فترجع حصانة الدم والمال إلى من كانوا من البغاة إذا انتهوا عن التمرد، ويترتب على ذلك قيام المسؤولية الجنائية على كل من يتعدى على أحدهم سواء كان من السلطة أو المواطنين[2].

وبناء على ذلك فإن جريمتي الحرابة والبغي في الشريعة الإسلامية يتوافقان مع صور الإرهاب الحديث[3]، وهو ما يستدعي تسليط العقوبات الحدية على التصرفات الإرهابية الحديثة إذا اشتملت على أركان جريمة الحرابة أو البغي وذلك بتخيير الحاكم وفق ما يراه مناسبا.

المطلب الرابع: حكم الإرهاب الإلكتروني.

لقد أثبت الواقع أن الجماعات الإرهابية هي من أكثر الفئات استخداما للتقنيات الحديثة والأكثر استغلالا لمعطيات التكنولوجيا ابتداء من نشرهم لفكر الإرهاب وتمجيده، مستخدمين في ذلك وسائل التواصل الاجتماعي ومواقع الانترنت والبريد الإلكتروني لتحقيق أهدافهم الضالة عبر الشبكة العالمية، وهو ما أرّق المجتمعات الإنسانية على اختلاف مللها وتنوع نظمها بما في ذلك الدول الإسلامية.

والمتعقب لأهداف وصور الإرهاب الإلكتروني المتعددة ـــ كجريمة إلكترونية[4] ـــ يجدها تستهدف المعلومات بأنواعها كمحل للجريمة، كما تستهدف الأموال والأشخاص والحكومات

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

وغيرها معتمدة في ذلك على التقنيات الحديثة لتنفيذ الجرائم الإرهابية، وعلى هذا الأساس فإن الإرهاب الإلكتروني لا يختلف عن الإرهاب التقليدي من حيث المقاصد بل يعد أكثر ضراوة من نظيره باعتبار الخصائص التي يتمتع بها جراء التكنولوجيا الحديثة والتي كان يفتقد إليها الإرهاب التقليدي، وهو ما أدى إلى إلحاق أكبر حد ممكن من الأضرار بالأفراد و المجتمعات والدول، بينما يكمن الفارق الأساسي بين ظاهرة الإرهاب التقليدي والإلكتروني في الوسيلة المستعملة لتحقيق ونشر الجريمة الإرهابية.

وعلى ضوء ذلك فإن الحكم الشرعي للإرهاب التقليدي ينصّب أيضا على الإرهاب الإلكتروني باعتبار التحريم، مما يجعل مجرمي الإرهاب الإلكتروني يخضعون للعقوبات الحدية إذا اجتمعت في تصرفاتهم شروط الحرابة أو البغي، كما لا يسلم دون ذلك من حكم التعزير الذي يكون تحديده من صلاحيات الإمام، وهو ما بادرت إليه العديد من الدول الإسلامية لردع هذه الظاهرة حيث فرضت عقوبات تعزيرية تتعلق بالإرهاب الإلكتروني، ومنها على سبيل المثال المملكة العربية السعودية التي نصت في المادة السابعة من قانون مكافحة جرائم المعلوماتية ما يلي:[1]

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1 ــ إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

2 ــ الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

ومثال ذلك أيضا، ما نص عليه القانون الاتحادي لدولة الإمارات العربية المتحدة رقم (2) الصادر سنة 2006 في شأن مكافحة جرائم تقنية المعلومات الإماراتي، في المواد التالية:[2]

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

المادة 20: كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة يعاقب بالحبس مدة لا تزيد على خمس سنوات.

المادة 21: كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد على خمس سنوات.

المادة 22: يعاقب بالسجن كل من دخل وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك.

فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها، تكون العقوبة السجن مدة لا تقل عن خمس سنوات.

ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

المادة 23: كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها.

والخلاصة أن الإرهاب الإلكتروني بجميع صوره محرم شرعا، وتتفاوت عقوبته بين التعزير والعقوبات الحدية إذا اجتمعت فيه شروط الحرابة أو البغي.

والله أعلم

---

(1) الإحالات في النسخة المطبوعة.

(2) الإحالات في النسخة المطبوعة.

...../...

الخاتمة

في ختام بحثي الموسوم بـــ " الجريمة الإلكترونية في الفقه الجنائي الإسلامي" تتجلى آثاره في كون الفقه الإسلامي لم يقف يوما أمام ما يستجد من الحوادث، فقد جاء بنظم متكاملة تتماشى وتطور المجتمعات واختلاف ظروفها حيث تضمن أصولا وقواعد تصلح لمواجهة كل أوضاع الحياة وظروف الزمان والمكان، كقاعدة " لا ضرر ولا ضرار"، وقاعدة "سد الذرائع"، وقاعدة "دفع المفاسد مقدم على جلب المصالح"، كما خول لولي الأمر تقرير العقوبات للجرائم غير الحدية والمستجدة منها مراعاة للمصلحة العامة للمجتمع، ونص على عقوبات محددة لا تتأثر باختلاف الأوضاع والظروف، وبذلك جمعت الشريعة الإسلامية في التجريم والعقاب بين الثابت والمرن والأصالة.

فمرونة الشريعة الإسلامية يجعلها صالحة لكل زمان ومكان ولكل ما هو مستحدث من أفعال وتصرفات لم تعهد من قبل، ولذلك فإن كل فعل مناف لتعاليم الدين الإسلامي يعاقب عليه لأن أساس اعتبار الفعل جريمة في نظر الإسلام هو مخالفة أوامر الدين[1]، وبذلك تكون الشريعة الإسلامية قد حددت إطار عام للأفعال المقبولة وغير المقبولة حديثها وقديمها، وهو سر تفوق التشريع الإسلامي على القوانين الوضعية.

وفي ضوء مقصد الشريعة الإسلامية من تحقيق المصالح التي تقوم على جلب المنافع ودرء المفاسد فإن الإسلام يمنع استخدام وسائل التكنولوجيا الحديثة بما فيها الحواسيب والانترنت في ارتكاب المحرمات وعلى رأسها الجرائم الإلكترونية وذلك استنادا إلى القاعدة الفقهية المستنبطة من النصوص الشرعية "تعطى الوسائل حكم الغايات"[2] فالوسائل في الفقه الإسلامي لها أحكام المقاصد، فما لا يتم الواجب إلا به فهو واجب، وما لا يتم المسنون إلا به فهو مسنون، وطرق الحرام والمكروهات تابعة لها، ووسيلة المباح مباحة.

---

(1) ـــ محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي، دار الفكر العربي، 1976م، القاهرة، ص: 31.

(2) ـــ محمد بكر إسماعيل، القواعد الفقهية بين الأصالة والتوجيه، دار المنار للطبع والنشر والتوزيع، القاهرة، مصر، ب.ت. ص: 116.

وقد توصلت من خلال البحث إلى النتائج التالية:

ـــ أن التشريع الإسلامي للعقوبات سواء في الحدود أو القصاص أوالتعازير مهمته الأولى رعاية مصلحة الأمة، وهي عامة على جميع أفرادها ولا تخضع في إقامتها لغضب سلطان ولا هواه.

ـــ أن العقوبات التعزيرية تقع على المعاصي التي لم يشرع فيها حد ولا كفارة ثابتة في الكتاب والسنة والإجماع والمعقول، وإنما فوض ولي الأمر أو من يقوم مقامه في تحديد نوعها وقدرها، حسب ظروف الجاني وملابسات الجريمة وآثارها على المجتمع.

ـــ أن آثار الجرائم الإلكترونية تطول جميع نواحي الحياة الاقتصادية منها والسياسية والاجتماعية والأمنية، كما لها آثار بليغة على المنظومة الأخلاقية للمجتمع الإسلامي.

ـــ أن البيانات والمعلومات والبرمجيات بأنواعها هي من الأموال المتقومة في الفقه الإسلامي، فيحرم التعدي عليها بأي وجه كان.

ـــ أن الحرز في الفقه الإسلامي يرجع إلى العرف السائد في الزمان والمكان.

ـــ أن اختراق الحواسيب والشبكات عن طريق كسر أنظمة حمايتها يعد انتهاك لحرز الأنظمة.

ـــ بالإمكان تسليط العقوبة الحدية على جرائم اختلاس الأموال عن طريق الحواسيب إذا ثبت للقاضي أن انتهاك أنظمة الحماية البرامجية هو انتهاك للحرز، مع تحقق باقي شروط السرقة الحدية.

ـــ تمتد الأنشطة الجرمية عبر الانترنت إلى العديد من الجرائم التقليدية كالمخدرات، والجريمة المنظمة، والتجارة غير المشروعة للأسلحة، والفساد السياسي والإداري والمالي، وتجارة الدعارة وغسل الأموال والإرهاب والتجسس، ولذلك فإن العديد منها يندرج ضمن العقوبات الحدية إذا استوفت شروطها وأركانها كجريمة القذف، والحرابة، والبغي.

ـــ تتضارب الجهود الوطنية والدولية في العالم الإسلامي لعدم توحدها في القضاء على الظاهرة خاصة من الناحية التشريعية، حيث أن كل دولة تتسم بقانون تشريعي خاص بها له اعتبارات بالسيادة

الوطنية وهو ما زاد من تفاقم ظاهرة الجريمة الإلكترونية لغياب النص التشريعي الموحد، رغم أن حل المعضلة متوفر في التشريع الجنائي الإسلامي.

وأود أن أشير إلى أنني لم آل جهدا، و لم أدخر وسعا في كتابة هذا البحث، ومع ذلك يبقى جهدي جهد المقل، حيث أنني لا أدعي له الكمال، بل أقر بأن الخطأ والنقصان صفتان متلازمتان لهذا الجهد المتواضع كسائر الجهود البشرية، والله الموفق للصواب.

التوصيات المقترحة:

أولا: ضرورة اهتمام العلماء والباحثين المسلمين بظاهرة الجريمة الإلكترونية باعتبارها أحد فروض الكفاية المستعجلة.

ثانيا: ضرورة الدعوة إلى عقد مؤتمر إسلامي دولي بمشاركة المنظمات الدولية ذات العلاقة، لوضع سياسات تشريعية نموذجية موحدة تعتمد على مصادر التشريع الإسلامي للتصدي للظاهرة.

ثالثا: إنشاء منظمة إسلامية تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الانترنت، مع تشجيع قيام اتحادات إسلامية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات في مواجهة الظاهرة.

رابعا: التأكيد على أهمية توثيق الروابط مع مراكز الدراسات والبحوث الأمنية والتقنية والقانونية في مختلف الدول خاصة في مجال نشر وتبادل نتائج الدراسات والبحوث المتعلقة بأمن المعلومات.

خامسا: ضرورة تفعيل التعاون الدولي فيما يتعلق بمكافحة الجرائم الإلكترونية، والاستفادة من تجارب بعض الدول المتقدمة التي حققت نتائج إيجابية في مواجهة الظاهرة.

سادسا: استحداث وحدات متخصصة في التحقيق والتحري في جرائم نظم المعلومات وجرائم شبكات الانترنت لتدعيم أجهزة العدالة الجنائية المعنية بمكافحة الجرائم الإلكترونية بمختلف صورها،

مع تفعيل دور الشرطة المجتمعية في مجال نشر الوعي المجتمعي الكفيل بمحاصرة جرائم تكنولوجيا المعلومات وتأكيد الاستخدام الأمثل لها.

سابعا: ضرورة إسهام الإعلام بجميع صوره بما في ذلك الخطب المسجدية للتبصير بأنواع الجرائم الإلكترونية والحذر منها خاصة لدى الناشئة الذين قد يغرر بهم، وتحذير الناس من مخاطرها وبيان أضرارها وطرق الوقاية منها، ونشر مفاهيم الرقابة الذاتية لدى المسلمين خاصة الشباب منهم عند التعامل مع التقنية الحديثة.

ثامنا: تفعيل دور الأسرة في متابعة الأبناء، لوقايتهم من الآثار السلبية، والمخاطر المترتبة على الاستخدام غير الآمن لشبكات الانترنت.

الفهارس العامة

فهرس الآيات القرآنية الكريمة

فهرس الأحاديث النبوية الشريفة

فهرس الجداول

فهرس الأشكال والبيانات

فهرس المصادر والمراجع

فهرس الآيات

الآيـــــة	رقمهـــا	الصفحـــة
﴿ سورة البقرة ﴾		
﴿ فَمَنِ ٱضْطُرَّ غَيْرَ بَاغٍ وَلَا عَادٍ فَلَآ إِثْمَ عَلَيْهِۚ ﴾	173	13
﴿وَأَقِيمُواْ ٱلصَّلَوٰةَ...﴾	43	29
﴿ لَا يُكَلِّفُ ٱللَّهُ نَفْسًا إِلَّا وُسْعَهَاۚ ﴾	286	32
﴿ يُرِيدُ ٱللَّهُ بِكُمُ ٱلْيُسْرَ وَلَا يُرِيدُ بِكُمُ ٱلْعُسْرَ ﴾	185	311_32
		347
﴿ وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ ﴾	188	304_294
		328_307
		399_366
﴿ إِنَّ ٱلَّذِينَ يَكْتُمُونَ مَآ أَنزَلْنَا مِنَ ٱلْبَيِّنَٰتِ وَٱلْهُدَىٰ مِنۢ بَعْدِ مَا بَيَّنَّٰهُ لِلنَّاسِ فِى ٱلْكِتَٰبِ أُوْلَٰٓئِكَ يَلْعَنُهُمُ ٱللَّهُ وَيَلْعَنُهُمُ ٱللَّٰعِنُونَ ﴾	159	299
﴿ وَلَا تَعْتَدُوٓاْۚ إِنَّ ٱللَّهَ لَا يُحِبُّ ٱلْمُعْتَدِينَ ﴾	190	312_306
﴿ وَإِذَا تَوَلَّىٰ سَعَىٰ فِى ٱلْأَرْضِ لِيُفْسِدَ فِيهَا وَيُهْلِكَ ٱلْحَرْثَ وَٱلنَّسْلَۗ وَٱللَّهُ لَا يُحِبُّ ٱلْفَسَادَ ﴾	205	306
﴿ فَمَنِ ٱعْتَدَىٰ عَلَيْكُمْ فَٱعْتَدُواْ عَلَيْهِ بِمِثْلِ مَا ٱعْتَدَىٰ عَلَيْكُمْۚ﴾	194	400
﴿ وَأَوْفُواْ بِعَهْدِىٓ أُوفِ بِعَهْدِكُمْ وَإِيَّٰىَ فَٱرْهَبُونِ ﴾	40	405
ذَٰلِكَ تَخْفِيفٌ مِّن رَّبِّكُمْ وَرَحْمَةٌۗ فَمَنِ ٱعْتَدَىٰ بَعْدَ ذَٰلِكَ فَلَهُۥ عَذَابٌ أَلِيمٌ ﴿١٧٨﴾ ﴾	178	408
﴿ سورة آل عمران ﴾		
﴿ وَلْتَكُن مِّنكُمْ أُمَّةٌ يَدْعُونَ إِلَى ٱلْخَيْرِ وَيَأْمُرُونَ بِٱلْمَعْرُوفِ وَيَنْهَوْنَ عَنِ ٱلْمُنكَرِۚ ﴾	104	315
﴿ وَمَا ٱللَّهُ يُرِيدُ ظُلْمًا لِّلْعَٰلَمِينَ ﴾	108	325
﴿ وَمِنْ أَهْلِ ٱلْكِتَٰبِ مَنْ إِن تَأْمَنْهُ بِقِنطَارٍ يُؤَدِّهِۦٓ إِلَيْكَ وَمِنْهُم مَّنْ إِن تَأْمَنْهُ بِدِينَارٍ لَّا يُؤَدِّهِۦٓ إِلَيْكَ إِلَّا مَا دُمْتَ عَلَيْهِ قَآئِمًاۚ ﴾	75	330

الآيـــــة	رقمهـــا	الصفحـة
﴿ سورة النساء ﴾		
﴿ إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ ﴾	58	9
﴿مَّن يُطِعِ ٱلرَّسُولَ فَقَدۡ أَطَاعَ ٱللَّهَۖ﴾	80	30
﴿يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَأۡكُلُوٓاْ أَمۡوَٰلَكُم بَيۡنَكُم بِٱلۡبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٖ مِّنكُمۡۚ﴾	29	307 ـ 335 349 ـ 366 400
﴿ وَإِذَا جَآءَهُمۡ أَمۡرٞ مِّنَ ٱلۡأَمۡنِ أَوِ ٱلۡخَوۡفِ أَذَاعُواْ بِهِۦۖ وَلَوۡ رَدُّوهُ إِلَى ٱلرَّسُولِ وَإِلَىٰٓ أُوْلِي ٱلۡأَمۡرِ مِنۡهُمۡ لَعَلِمَهُ ٱلَّذِينَ يَسۡتَنۢبِطُونَهُۥ مِنۡهُمۡۗ وَلَوۡلَا فَضۡلُ ٱللَّهِ عَلَيۡكُمۡ وَرَحۡمَتُهُۥ لَٱتَّبَعۡتُمُ ٱلشَّيۡطَٰنَ إِلَّا قَلِيلٗا ﴾	83	315
﴿ إِنَّ ٱللَّهَ لَا يَغۡفِرُ أَن يُشۡرَكَ بِهِۦ وَيَغۡفِرُ مَا دُونَ ذَٰلِكَ لِمَن يَشَآءُۚ وَمَن يُشۡرِكۡ بِٱللَّهِ فَقَدِ ٱفۡتَرَىٰٓ إِثۡمًا عَظِيمًا ﴾	48	323
﴿ إِنَّ ٱلَّذِينَ يَأۡكُلُونَ أَمۡوَٰلَ ٱلۡيَتَٰمَىٰ ظُلۡمًا إِنَّمَا يَأۡكُلُونَ فِي بُطُونِهِمۡ نَارٗاۖ وَسَيَصۡلَوۡنَ سَعِيرٗا﴾	10	400
﴿ وَمَن يَقۡتُلۡ مُؤۡمِنٗا مُّتَعَمِّدٗا فَجَزَآؤُهُۥ جَهَنَّمُ خَٰلِدٗا فِيهَا ﴾	93	408
﴿ سورة المائدة ﴾		
﴿وَٱتۡلُ عَلَيۡهِمۡ نَبَأَ ٱبۡنَيۡ ءَادَمَ بِٱلۡحَقِّ إِذۡ قَرَّبَا قُرۡبَانٗا فَتُقُبِّلَ مِنۡ أَحَدِهِمَا وَلَمۡ يُتَقَبَّلۡ مِنَ ٱلۡأٓخَرِ قَالَ لَأَقۡتُلَنَّكَۖ قَالَ إِنَّمَا يَتَقَبَّلُ ٱللَّهُ مِنَ ٱلۡمُتَّقِينَ ٢٧ لَئِنۢ بَسَطتَ إِلَيَّ يَدَكَ لِتَقۡتُلَنِي مَآ أَنَا۠ بِبَاسِطٖ يَدِيَ إِلَيۡكَ لِأَقۡتُلَكَۖ إِنِّيٓ أَخَافُ ٱللَّهَ رَبَّ ٱلۡعَٰلَمِينَ ٢٨ إِنِّيٓ أُرِيدُ أَن تَبُوٓأَ بِإِثۡمِي وَإِثۡمِكَ فَتَكُونَ مِنۡ أَصۡحَٰبِ ٱلنَّارِۚ وَذَٰلِكَ جَزَٰٓؤُاْ ٱلظَّٰلِمِينَ ٢٩ فَطَوَّعَتۡ لَهُۥ نَفۡسُهُۥ قَتۡلَ أَخِيهِ فَقَتَلَهُۥ فَأَصۡبَحَ مِنَ ٱلۡخَٰسِرِينَ ٣٠﴾	27 — 30	أ
﴿وَلَا يَجۡرِمَنَّكُمۡ شَنَـَٔانُ قَوۡمٍ﴾	8	4
﴿ لَئِنۡ أَقَمۡتُمُ ٱلصَّلَوٰةَ وَءَاتَيۡتُمُ ٱلزَّكَوٰةَ وَءَامَنتُم بِرُسُلِي وَعَزَّرۡتُمُوهُمۡ وَأَقۡرَضۡتُمُ ٱللَّهَ قَرۡضًا حَسَنٗا لَّأُكَفِّرَنَّ عَنكُمۡ سَيِّـَٔاتِكُمۡ وَلَأُدۡخِلَنَّكُمۡ جَنَّٰتٖ تَجۡرِي مِن تَحۡتِهَا ٱلۡأَنۡهَٰرُۚ﴾	12	6
﴿وَإِذَا حَلَلۡتُمۡ فَٱصۡطَادُواْۚ ﴾	2	9
﴿وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقۡطَعُوٓاْ أَيۡدِيَهُمَا﴾	38	10 ـ 290 400

الآيـــــة	رقمهـــا	الصفحـة
﴿ وَكَتَبْنَا عَلَيْهِمْ فِيهَآ أَنَّ ٱلنَّفْسَ بِٱلنَّفْسِ وَٱلْعَيْنَ بِٱلْعَيْنِ وَٱلْأَنفَ بِٱلْأَنفِ وَٱلْأُذُنَ بِٱلْأُذُنِ وَٱلسِّنَّ بِٱلسِّنِّ وَٱلْجُرُوحَ قِصَاصٌ ﴾	45	36
﴿ مَا يُرِيدُ ٱللَّهُ لِيَجْعَلَ عَلَيْكُم مِّنْ حَرَجٍ وَلَٰكِن يُرِيدُ لِيُطَهِّرَكُمْ وَلِيُتِمَّ نِعْمَتَهُۥ عَلَيْكُمْ لَعَلَّكُمْ تَشْكُرُونَ ﴾	6	311
﴿ إِنَّمَا جَزَٰٓؤُاْ ٱلَّذِينَ يُحَارِبُونَ ٱللَّهَ وَرَسُولَهُۥ وَيَسْعَوْنَ فِى ٱلْأَرْضِ فَسَادًا أَن يُقَتَّلُوٓاْ أَوْ يُصَلَّبُوٓاْ أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُم مِّنْ خِلَٰفٍ أَوْ يُنفَوْاْ مِنَ ٱلْأَرْضِ ذَٰلِكَ لَهُمْ خِزْىٌ فِى ٱلدُّنْيَا وَلَهُمْ فِى ٱلْءَاخِرَةِ عَذَابٌ عَظِيمٌ ﴾	33	375_ 338 408_ 376 413
﴿يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَتَّخِذُواْ ٱلْيَهُودَ وَٱلنَّصَٰرَىٰٓ أَوْلِيَآءَ بَعْضُهُمْ أَوْلِيَآءُ بَعْضٍ وَمَن يَتَوَلَّهُم مِّنكُمْ فَإِنَّهُۥ مِنْهُمْ إِنَّ ٱللَّهَ لَا يَهْدِى ٱلْقَوْمَ ٱلظَّٰلِمِينَ ﴾	51	385
﴿ مِنْ أَجْلِ ذَٰلِكَ كَتَبْنَا عَلَىٰ بَنِىٓ إِسْرَٰٓءِيلَ أَنَّهُۥ مَن قَتَلَ نَفْسًۢا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِى ٱلْأَرْضِ فَكَأَنَّمَا قَتَلَ ٱلنَّاسَ جَمِيعًا ﴾	32	408
﴿ سورة الأنعام ﴾		
﴿مَّا فَرَّطْنَا فِى ٱلْكِتَٰبِ مِن شَىْءٍ﴾	38	31
﴿ وَلَا تَقْتُلُواْ ٱلنَّفْسَ ٱلَّتِى حَرَّمَ ٱللَّهُ إِلَّا بِٱلْحَقِّ ﴾	151	408_ 374
﴿ سورة الأعراف ﴾		
﴿ وَلَا تَبْخَسُواْ ٱلنَّاسَ أَشْيَآءَهُمْ ﴾	85	300
﴿وَلَا تُفْسِدُواْ فِى ٱلْأَرْضِ بَعْدَ إِصْلَٰحِهَا ﴾	56	306
﴿ وَلَمَّا سَكَتَ عَن مُّوسَى ٱلْغَضَبُ أَخَذَ ٱلْأَلْوَاحَ وَفِى نُسْخَتِهَا هُدًى وَرَحْمَةٌ لِّلَّذِينَ هُمْ لِرَبِّهِمْ يَرْهَبُونَ﴾	154	405
﴿ قُلْ إِنَّمَا حَرَّمَ رَبِّىَ ٱلْفَوَٰحِشَ مَا ظَهَرَ مِنْهَا وَمَا بَطَنَ وَٱلْإِثْمَ وَٱلْبَغْىَ بِغَيْرِ ٱلْحَقِّ ﴾	33	415
﴿ سورة الأنفال ﴾		
﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمْ وَأَنتُمْ تَعْلَمُونَ ﴾	27	385
﴿ وَأَعِدُّواْ لَهُم مَّا ٱسْتَطَعْتُم مِّن قُوَّةٍ وَمِن رِّبَاطِ ٱلْخَيْلِ تُرْهِبُونَ بِهِۦ عَدُوَّ ٱللَّهِ وَعَدُوَّكُمْ وَءَاخَرِينَ مِن دُونِهِمْ لَا تَعْلَمُونَهُمُ ٱللَّهُ يَعْلَمُهُمْ ﴾	60	407 _ 406

الآيـــــة	رقمهـــا	الصفحـة
﴿ سورة التوبة ﴾		
﴿فَلَوْلَا نَفَرَ مِن كُلِّ فِرْقَةٍ مِّنْهُمْ طَآئِفَةٌ لِّيَتَفَقَّهُواْ فِي ٱلدِّينِ وَلِيُنذِرُواْ قَوْمَهُمْ إِذَا رَجَعُوٓاْ إِلَيْهِمْ لَعَلَّهُمْ يَحْذَرُونَ ﴾	122	28
﴿ وَٱلَّذِينَ يَكْنِزُونَ ٱلذَّهَبَ وَٱلْفِضَّةَ وَلَا يُنفِقُونَهَا فِي سَبِيلِ ٱللَّهِ ﴾	34	330 ـ 406
﴿ ٱتَّخَذُوٓاْ أَحْبَارَهُمْ وَرُهْبَٰنَهُمْ أَرْبَابًا مِّن دُونِ ٱللَّهِ ﴾	31	406
﴿ سورة هود ﴾		
﴿وَيَٰقَوْمِ لَا يَجْرِمَنَّكُمْ شِقَاقِيٓ أَن يُصِيبَكُم مِّثْلُ مَآ أَصَابَ قَوْمَ نُوحٍ أَوْ قَوْمَ هُودٍ أَوْ قَوْمَ صَٰلِحٍ ۚ وَمَا قَوْمُ لُوطٍ مِّنكُم بِبَعِيدٍ﴾	89	4
﴿ سورة يوسف ﴾		
﴿ وَشَرَوْهُ بِثَمَنٍۭ بَخْسٍ دَرَٰهِمَ مَعْدُودَةٍ وَكَانُواْ فِيهِ مِنَ ٱلزَّٰهِدِينَ ﴾	20	330
﴿ قَالَ ٱجْعَلْنِي عَلَىٰ خَزَآئِنِ ٱلْأَرْضِ ۖ إِنِّي حَفِيظٌ عَلِيمٌ﴾	55	346
﴿ قَالَ رَبِّ ٱلسِّجْنُ أَحَبُّ إِلَيَّ مِمَّا يَدْعُونَنِيٓ إِلَيْهِ ۖ وَإِلَّا تَصْرِفْ عَنِّي كَيْدَهُنَّ أَصْبُ إِلَيْهِنَّ وَأَكُن مِّنَ ٱلْجَٰهِلِينَ ﴾	33	371
﴿ سورة إبراهيم ﴾		
﴿ رَبَّنَآ إِنَّكَ تَعْلَمُ مَا نُخْفِي وَمَا نُعْلِنُ ۗ ﴾	38	343
﴿ سورة النحل ﴾		
﴿فَسْـَٔلُوٓاْ أَهْلَ ٱلذِّكْرِ إِن كُنتُمْ لَا تَعْلَمُونَ﴾	43	ى
﴿ إِلَّا مَنْ أُكْرِهَ وَقَلْبُهُۥ مُطْمَئِنٌّۢ بِٱلْإِيمَٰنِ ﴾	106	13
﴿وَأَنزَلْنَآ إِلَيْكَ ٱلذِّكْرَ لِتُبَيِّنَ لِلنَّاسِ مَا نُزِّلَ إِلَيْهِمْ﴾	44	30
﴿ وَٱللَّهُ يَعْلَمُ مَا تُسِرُّونَ وَمَا تُعْلِنُونَ ﴾	19	343
﴿ وَلَا تَقُولُواْ لِمَا تَصِفُ أَلْسِنَتُكُمُ ٱلْكَذِبَ هَٰذَا حَلَٰلٌ وَهَٰذَا حَرَامٌ لِّتَفْتَرُواْ عَلَى ٱللَّهِ ٱلْكَذِبَ ۚ إِنَّ ٱلَّذِينَ يَفْتَرُونَ عَلَى ٱللَّهِ ٱلْكَذِبَ لَا يُفْلِحُونَ ﴾	116	349
﴿ وَقَالَ ٱللَّهُ لَا تَتَّخِذُوٓاْ إِلَٰهَيْنِ ٱثْنَيْنِ ۖ إِنَّمَا هُوَ إِلَٰهٌ وَٰحِدٌ فَإِيَّٰيَ فَٱرْهَبُونِ ﴾	51	405 ـ 406

الآيـــــة	رقمهـــا	الصفحـة
﴿ سورة الإسراء ﴾		
﴿ وَلَا تَقْتُلُواْ ٱلنَّفْسَ ٱلَّتِى حَرَّمَ ٱللَّهُ إِلَّا بِٱلْحَقِّ ﴾	33	9
﴿وَلَا تَقْرَبُواْ ٱلزِّنَىٰٓ إِنَّهُۥ كَانَ فَٰحِشَةً وَسَآءَ سَبِيلًا ﴾	32	9 ـ 374
		375
﴿ وَمَن قُتِلَ مَظْلُومًا فَقَدْ جَعَلْنَا لِوَلِيِّهِۦ سُلْطَٰنًا ﴾	33	9
﴿ وَإِن مِّن شَىْءٍ إِلَّا يُسَبِّحُ بِحَمْدِهِۦ وَلَٰكِن لَّا تَفْقَهُونَ تَسْبِيحَهُمْ ﴾	44	28
﴿ وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَىٰ ﴾	15	227
﴿ سورة الكهف ﴾		
﴿ تَّزَٰوَرُ عَن كَهْفِهِمْ ﴾	17	316
﴿ وَيُنذِرَ ٱلَّذِينَ قَالُواْ ٱتَّخَذَ ٱللَّهُ وَلَدًا ۝٤ مَّا لَهُم بِهِۦ مِنْ عِلْمٍ وَلَا لِءَابَآئِهِمْ كَبُرَتْ كَلِمَةً تَخْرُجُ		
مِنْ أَفْوَٰهِهِمْ إِن يَقُولُونَ إِلَّا كَذِبًا ﴾	4 ـ 5	348
﴿ قَالَ ذَٰلِكَ مَا كُنَّا نَبْغِ ﴾	64	415
﴿ سورة طه ﴾		
﴿ إِنَّهُۥ مَن يَأْتِ رَبَّهُۥ مُجْرِمًا فَإِنَّ لَهُۥ جَهَنَّمَ لَا يَمُوتُ فِيهَا وَلَا يَحْيَىٰ ۝٧٤ ﴾	74	أ
﴿ وَٱحْلُلْ عُقْدَةً مِّن لِّسَانِى ۝٢٧ يَفْقَهُواْ قَوْلِى ﴾	28ـ27	28
﴿ سورة الأنبياء ﴾		
﴿بَلْ نَقْذِفُ بِٱلْحَقِّ عَلَى ٱلْبَٰطِلِ فَيَدْمَغُهُۥ فَإِذَا هُوَ زَاهِقٌ ﴾	18	149
﴿ إِنَّهُمْ كَانُواْ يُسَٰرِعُونَ فِى ٱلْخَيْرَٰتِ وَيَدْعُونَنَا رَغَبًا وَرَهَبًا وَكَانُواْ لَنَا خَٰشِعِينَ ﴾	90	405 - 406
﴿ سورة الحج ﴾		
﴿ وَمَا جَعَلَ عَلَيْكُمْ فِى ٱلدِّينِ مِنْ حَرَجٍ ﴾	78	311ـ 347
﴿ فَٱجْتَنِبُواْ ٱلرِّجْسَ مِنَ ٱلْأَوْثَٰنِ وَٱجْتَنِبُواْ قَوْلَ ٱلزُّورِ ﴾	30	323ـ327

الآيـــــة	رقمهـــا	الصفحـة
﴿ سورة النور ﴾		
﴿ٱلزَّانِيَةُ وَٱلزَّانِي فَٱجْلِدُواْ كُلَّ وَٰحِدٍ مِّنْهُمَا مِاْئَةَ جَلْدَةٍ﴾	2	9
﴿لَّوْلَا جَآءُو عَلَيْهِ بِأَرْبَعَةِ شُهَدَآءَ فَإِذْ لَمْ يَأْتُواْ بِٱلشُّهَدَآءِ فَأُوْلَٰٓئِكَ عِندَ ٱللَّهِ هُمُ ٱلْكَٰذِبُونَ﴾	13	10
﴿ وَٱلَّذِينَ يَرْمُونَ ٱلْمُحْصَنَٰتِ ثُمَّ لَمْ يَأْتُواْ بِأَرْبَعَةِ شُهَدَآءَ فَٱجْلِدُوهُمْ ثَمَٰنِينَ جَلْدَةً وَلَا تَقْبَلُواْ لَهُمْ شَهَٰدَةً أَبَدًا وَأُوْلَٰٓئِكَ هُمُ ٱلْفَٰسِقُونَ ﴾	4	354
﴿ إِنَّ ٱلَّذِينَ يَرْمُونَ ٱلْمُحْصَنَٰتِ ٱلْغَٰفِلَٰتِ ٱلْمُؤْمِنَٰتِ لُعِنُواْ فِى ٱلدُّنْيَا وَٱلْءَاخِرَةِ وَلَهُمْ عَذَابٌ عَظِيمٌ ۝ يَوْمَ تَشْهَدُ عَلَيْهِمْ أَلْسِنَتُهُمْ وَأَيْدِيهِمْ وَأَرْجُلُهُم بِمَا كَانُواْ يَعْمَلُونَ ۝ يَوْمَئِذٍ يُوَفِّيهِمُ ٱللَّهُ دِينَهُمُ ٱلْحَقَّ وَيَعْلَمُونَ أَنَّ ٱللَّهَ هُوَ ٱلْحَقُّ ٱلْمُبِينُ ﴾	25 ـ 23	355
﴿ إِنَّ ٱلَّذِينَ يُحِبُّونَ أَن تَشِيعَ ٱلْفَٰحِشَةُ فِى ٱلَّذِينَ ءَامَنُواْ لَهُمْ عَذَابٌ أَلِيمٌ فِى ٱلدُّنْيَا وَٱلْءَاخِرَةِ وَٱللَّهُ يَعْلَمُ وَأَنتُمْ لَا تَعْلَمُونَ ﴾	19	368 ـ358 375
﴿ قُل لِّلْمُؤْمِنِينَ يَغُضُّواْ مِنْ أَبْصَٰرِهِمْ وَيَحْفَظُواْ فُرُوجَهُمْ ذَٰلِكَ أَزْكَىٰ لَهُمْ إِنَّ ٱللَّهَ خَبِيرٌ بِمَا يَصْنَعُونَ﴾	30	376 ـ 374
﴿ سورة الفرقان ﴾		
﴿فَقَدْ جَآءُو ظُلْمًا وَزُورًا﴾	4	324ـ123
﴿ وَٱلَّذِينَ لَا يَشْهَدُونَ ٱلزُّورَ وَإِذَا مَرُّواْ بِٱللَّغْوِ مَرُّواْ كِرَامًا ﴾	72	324
﴿ سورة القصص ﴾		
﴿ قَالَ أَلْقُواْ فَلَمَّآ أَلْقَوْاْ سَحَرُوٓاْ أَعْيُنَ ٱلنَّاسِ وَٱسْتَرْهَبُوهُمْ وَجَآءُو بِسِحْرٍ عَظِيمٍ﴾	32	405
﴿ سورة الأحزاب ﴾		
﴿ وَٱلَّذِينَ يُؤْذُونَ ٱلْمُؤْمِنِينَ وَٱلْمُؤْمِنَٰتِ بِغَيْرِ مَا ٱكْتَسَبُواْ فَقَدِ ٱحْتَمَلُواْ بُهْتَٰنًا وَإِثْمًا مُّبِينًا ﴾	58	358
﴿ سورة ص ﴾		
﴿ هَٰذَا مُغْتَسَلٌۢ بَارِدٌ وَشَرَابٌ ﴾	42	391

الآيـــــة	رقمهـــا	الصفحـة
﴿ سورة الزمر ﴾		
﴿قُلْ هَلْ يَسْتَوِى ٱلَّذِينَ يَعْلَمُونَ وَٱلَّذِينَ لَا يَعْلَمُونَ﴾	9	ب
﴿ سورة فصلت ﴾		
﴿ مَّنْ عَمِلَ صَٰلِحًا فَلِنَفْسِهِۦ وَمَنْ أَسَآءَ فَعَلَيْهَا ﴾	46	227
﴿ وَمَا رَبُّكَ بِظَلَّٰمٍ لِّلْعَبِيدِ ﴾	46	325
﴿ سورة الشورى ﴾		
﴿إِنَّمَا ٱلسَّبِيلُ عَلَى ٱلَّذِينَ يَظْلِمُونَ ٱلنَّاسَ وَيَبْغُونَ فِى ٱلْأَرْضِ بِغَيْرِ ٱلْحَقِّ أُو۟لَٰٓئِكَ لَهُمْ عَذَابٌ أَلِيمٌ﴾	42	417
﴿ سورة الزخرف ﴾		
﴿إِنَّ ٱلْمُجْرِمِينَ فِى عَذَابِ جَهَنَّمَ خَٰلِدُونَ ﴿٧٤﴾ لَا يُفَتَّرُ عَنْهُمْ وَهُمْ فِيهِ مُبْلِسُونَ ﴿٧٥﴾ وَمَا ظَلَمْنَٰهُمْ وَلَٰكِن كَانُوا۟ هُمُ ٱلظَّٰلِمِينَ ﴿٧٦﴾ وَنَادَوْا۟ يَٰمَٰلِكُ لِيَقْضِ عَلَيْنَا رَبُّكَ ۖ قَالَ إِنَّكُم مَّٰكِثُونَ ﴿٧٧﴾ لَقَدْ جِئْنَٰكُم بِٱلْحَقِّ وَلَٰكِنَّ أَكْثَرَكُمْ لِلْحَقِّ كَٰرِهُونَ ﴿٧٨﴾ أَمْ أَبْرَمُوٓا۟ أَمْرًا فَإِنَّا مُبْرِمُونَ ﴿٧٩﴾ أَمْ يَحْسَبُونَ أَنَّا لَا نَسْمَعُ سِرَّهُمْ وَنَجْوَىٰهُم ۚ بَلَىٰ وَرُسُلُنَا لَدَيْهِمْ يَكْتُبُونَ ﴿٨٠﴾﴾	74 — 80	4
﴿ سورة الحجرات ﴾		
﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوا۟ ٱجْتَنِبُوا۟ كَثِيرًا مِّنَ ٱلظَّنِّ إِنَّ بَعْضَ ٱلظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا۟ وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَٱتَّقُوا۟ ٱللَّهَ ۚ إِنَّ ٱللَّهَ تَوَّابٌ رَّحِيمٌ ﴾	12	359_160 379 _ 366 389_ 383
﴿وَإِن طَآئِفَتَانِ مِنَ ٱلْمُؤْمِنِينَ ٱقْتَتَلُوا۟ فَأَصْلِحُوا۟ بَيْنَهُمَا ۖ فَإِنۢ بَغَتْ إِحْدَىٰهُمَا عَلَى ٱلْأُخْرَىٰ فَقَٰتِلُوا۟ ٱلَّتِى تَبْغِى حَتَّىٰ تَفِىٓءَ إِلَىٰٓ أَمْرِ ٱللَّهِ ۚ فَإِن فَآءَتْ فَأَصْلِحُوا۟ بَيْنَهُمَا بِٱلْعَدْلِ وَأَقْسِطُوٓا۟ ۖ إِنَّ ٱللَّهَ يُحِبُّ ٱلْمُقْسِطِينَ﴾	9	417_415

الآيـــــة	رقمهـــا	الصفحـة
﴿ سورة النجم ﴾		
﴿ وَأَن لَّيْسَ لِلْإِنسَٰنِ إِلَّا مَا سَعَىٰ ۝ وَأَنَّ سَعْيَهُۥ سَوْفَ يُرَىٰ ﴾	39 ـ 40	300
﴿ فَلَا تُزَكُّوٓاْ أَنفُسَكُمْۖ هُوَ أَعْلَمُ بِمَنِ ٱتَّقَىٰٓ﴾	32	346
﴿ سورة الحديد ﴾		
﴿وَجَعَلْنَا فِى قُلُوبِ ٱلَّذِينَ ٱتَّبَعُوهُ رَأْفَةً وَرَحْمَةً ۚ وَرَهْبَانِيَّةً ٱبْتَدَعُوهَا مَا كَتَبْنَٰهَا عَلَيْهِمْ إِلَّا ٱبْتِغَآءَ رِضْوَٰنِ ٱللَّهِ فَمَا رَعَوْهَا حَقَّ رِعَايَتِهَاۖ فَـَٔاتَيْنَا ٱلَّذِينَ ءَامَنُواْ مِنْهُمْ أَجْرَهُمْۖ وَكَثِيرٌ مِّنْهُمْ فَٰسِقُونَ ﴾	27	406
﴿ سورة المجادلة ﴾		
﴿ وَإِنَّهُمْ لَيَقُولُونَ مُنكَرًا مِّنَ ٱلْقَوْلِ وَزُورًا ۚ وَإِنَّ ٱللَّهَ لَعَفُوٌّ غَفُورٌ ﴾	2	324
﴿ سورة الحشر ﴾		
﴿ لَأَنتُمْ أَشَدُّ رَهْبَةً فِى صُدُورِهِم مِّنَ ٱللَّهِۚ ذَٰلِكَ بِأَنَّهُمْ قَوْمٌ لَّا يَفْقَهُونَ ﴾	13	405
﴿ سورة المنافقون ﴾		
﴿إِذَا جَآءَكَ ٱلْمُنَٰفِقُونَ قَالُواْ نَشْهَدُ إِنَّكَ لَرَسُولُ ٱللَّهِۘ وَٱللَّهُ يَعْلَمُ إِنَّكَ لَرَسُولُهُۥ وَٱللَّهُ يَشْهَدُ إِنَّ ٱلْمُنَٰفِقِينَ لَكَٰذِبُونَ ۝ ٱتَّخَذُوٓاْ أَيْمَٰنَهُمْ جُنَّةً فَصَدُّواْ عَن سَبِيلِ ٱللَّهِۚ ﴾	1 - 2	11
﴿ سورة الحاقة ﴾		
﴿ وَلَا طَعَامٌ إِلَّا مِنْ غِسْلِينٍ ۝ لَّا يَأْكُلُهُۥٓ إِلَّا ٱلْخَٰطِـُٔونَ ﴾	36 ـ 37	391
﴿ سورة الجن ﴾		
﴿ وَأَنَّا لَمَسْنَا ٱلسَّمَآءَ ﴾	8	379

فهرس الأحاديث

الحديث **الصفحة**

﴿ أ ﴾

- إذا أردت مضجعك فقل: اللهم أسلمت نفسي إليك، وفوضت أمري إليك، ووجهت وجهي إليك، وألجأت ظهري إليك رغبة ورهبة إليك، لا ملجأ إلا إليك، آمنت بكتابك الذي أنزلت وبنبيك الذي أرسلت، فإن مت مت على الفطرة 407
- إذا حدث الرجل بالحديث ثم التفت فهي أمانة 385
- اجتنبوا السبع الموبقات، قالوا وما هن يا رسول الله؟ قال: الشرك بالله، والسحر، وقتل النفس التي حرم الله إلا بالحق، وأكل الربا، وأكل مال اليتيم، والتولي يوم الزحف، وقذف المحصنات الغافلات 356
- إذا مات ابن آدم انقطع عمله إلا من ثلاث؛ وذكر منها: علم ينتفع به... 301
- أفلا جعلته فوق الطعام حتى يراه الناس، من غش فليس منا 347
350
ألا أنبئكم بأكبر الكبائر؟ قلنا: بلى يا رسول الله، قال: الإشراك بالله وعقوق الوالدين، وكان متكئا فجلس، فقال: ألا وقول الزور وشهادة الزور، فما زال يكررها حتى قلنا ليته سكت 324
- ألا إني أوتيت القرآن ومثله معه 30
- إن الله تعالى تجاوز لأمتي عما وسوست أو حدثت به أنفسها ما لم تعمل أو تتكلم 11
- إن الله حرم عليكم دماءكم وأموالكم كحرمة يومكم هذا ، في بلدكم هذا في شهركم هذا ، ألا هل بلغت ؟ قالوا : نعم ، قال : اللهم اشهد 335
- إن الله كتب الحسنات والسيئات ثم بين ذلك فمن هم بحسنة فلم يعملها كتبها الله له عنده حسنة كاملة فإن هو هم بها فعملها كتبها الله له عنده عشر حسنات إلى سبع مائة ضعف إلى أضعاف كثيرة، ومن هم بسيئة فلم يعملها كتبها الله له عنده حسنة كاملة فإن هو هم بها فعملها كتبها الله له سيئة واحدة 11
- إن دماءكم وأموالكم حرام عليكم، كحرمة يومكم هذا، في شهركم هذا، في بلدكم هذا 307
- إنك إن اتبعت عورات الناس أفسدتهم أو كدت أن تفسدهم 368
- إنما أنا بشر وإنكم تختصمون إليّ، ولعل بعضكم أن يكون ألحن بحجته من بعض فأقضي له على نحو ما أسمع، فمن قضيت له بحق مسلم، فإنما هي قطعة من النار فليأخذها أو ليتركها 31
- إنه ستكون هَنَاتٌ وهَنَاتٌ وهناتٌ، فمن أراد أن يفرق أمر المسلمين وهم جميع فاضربوه بالسيفِ كائنًا من كان 417
- إياكم والظن فإن الظن أكذب الحديث ولا تجسسوا ولا تحسسوا ولا تناجشوا ولا تحاسدوا ولا تباغضوا ولا تدابروا وكونوا عباد الله إخوانا 368
379
383
389

﴿ب﴾

- البينة على المدعي واليمين على من أنكر 30

﴿ت﴾

- التاجر الصدوق الأمين يحشر يوم القيامة مع النبيين والصديقين والشهداء 348
- التجار يحشرون يوم القيامة فجارا إلا من اتقى الله وبر وصدق 349
- تقطع اليد في ربع دينار فصاعدا 335

﴿ر﴾

- رفع القلم عن ثلاث، عن الصبي حتى يبلغ، وعن النائم حتى يستيقظ، وعن المجنون حتى يفيق 12
- رفع عن أمتي الخطأ والنسيان 13

﴿ع﴾

- عليكم بالصدق، فإنه يهدي إلى البر وإن البر يهدي إلى الجنة، وإن الرجل ليصدق حتى يكتب عند الله صديقا، وإياكم والكذب، فإن الكذب يهدي إلى الفجور، وإن الفجور يهدي إلى النار، وإن الرجل ليكذب حتى يكتب عند الله كذابا 349
- العينان تزنيان وزناهما النظر 374

﴿ف﴾

- فإن دماءكم وأموالكم وأعراضكم عليكم حرام، كحرمة يومكم هذا، في بلدكم هذا في شهركم هذا، وأعادها مرارا، ثم رفع رأسه، فقال اللهم هل بلغت... 353
400

﴿ك﴾

- كل المسلم على المسلم حرام، دمه وماله وعرضه 307
367

﴿ ل ﴾

- لا تُبَاشِرُ الْمَرْأَةُ الْمَرْأَةَ فَتَنْعَتَهَا لِزَوْجِهَا كَأَنَّهُ يَنْظُرُ إِلَيْهَا 374
- لا تصرّوا الإبل والغنم، فمن ابتاعها بعد فإنه بِخير النظرَيْنِ بعدَ أن يحتلبها: إن شاء أمسك، وإن شاء ردّها وصاع تمر 350
- لا تقطع اليد إلا في ربع دينار فما فوقه 10
- لا ضرر ولا ضرار 29
302
306
395
- لا قطع في ثمر معلق 10
- لا ميراث لقاتل 10
- لا يحل مال امرئ مسلم إلا بطيب من نفسه 301
304
- لا يحل لأحدكم أن يأخذ متاع أخيه لاعبا ولا جادا، فإن أخذه فليرده عليه 401
- لا يزني الزاني حين يزني وهو مؤمن، ولا يشرب الخمر حين يشربها وهو مؤمن، ولا يسرق السارق حين يسرق وهو مؤمن 290
- لو أن امرأ اطلع عليك بغير إذن فحذفته بحصاة ففقأت عينه لم يكن عليه جناح 368
- لا يؤخذ الرجل بجريرة أبيه ولا بجريرة أخيه 227
- ليس على الخائن ولا المختلس قطع 336
- ليس على خائن ولا منتهب ولا مختلس قطع 293

﴿ م ﴾

- ما أخذ في غير أكمامه فاحتمل ففيه قيمته ومثله معه، وما كان في الجرين ففيه القطع إذا بلغ ثمن المجن 336
- ما بعث الله من نبي ولا استخلف خليفة إلا كانت له بطانتان: بطانة تأمره بالمعروف وتحضه عليه، وبطانة تأمره بالشر وتحضه عليه والمعصوم من عَصَمَ الله تعالى 382
- ما من امرئ يخذل امرأ مسلما في موضع تنتهك فيه حرمته، وينتقص فيه من عرضه إلا خذله الله تعالى في موطن يحب فيه نصرته، وما من امرئ ينصر امرأ مسلما في موضع ينتقص فيه من عرضه وينتهك فيه من حرمته إلا نصره الله عز وجل في موطن يحب فيه نصرته 385
- ما من رجل يحفظ علما فيكتمه، إلا أتى به يوم القيامة ملجما من النار 299
- المسلمون على شروطهم 301
304

- من خرج من الطاعة وفارق الجماعة فمات، مات ميتة جاهلية، ومن قاتل تحت راية عمية يغضب لعصبة أو يدعو إلى عصبة أو ينصر عصبة فقتل، فقِتلة جاهلية، ومن خرج على أمتي يضر برها وفاجرها ولا يتحاشى من مؤمنها ولا يفي لذي عهد عهده فليس مني ولست منه 417
- من رأى منكم منكراً فليغيره بيده، فإن لم يستطع فبلسانه فإن لم يستطع فبقلبه، وذلك أضعف الإيمان 315
- من سبق إلى ما لم يسبق إليه مسلم فهو له 302
- من سبق إلى مباح فهو أحق به 305
- من ستر عورة مؤمن فكأنما استحيا موؤدة من قبرها 384
- من سمّع سمّع الله به، ومن يُرائي يُرائي الله به 360
- من ستر مسلما ستره الله عز وجل يوم القيامة 360
- من ضار ضار الله به ومن شاق شاق الله عليه 306
- من غشنا فليس منا 327
- (من يرد الله به خيراً يفقهه في الدين) 28

﴿ ي ﴾

- يا معشر من قد أسلم بلسانه و لم يفض الإيمان إلى قلبه، لا تؤذوا المسلمين، ولا تعيروهم، ولا تتبعوا عوراتهم، فإنه من تتبع عورة أخيه المسلم تتبع الله عورته، ومن تتبع الله عورته يفضحه، ولو في جوف رحله 359
- يا أسامة: سر على اسم الله، وبركته، حتى تنتهي إلى مقتل أبيك، فأوطئهم الخيل، فقد وليتك هذا الجيش، فأغر صباحا على أهل أبنا ـــ أبنى ـــ وحرّق عليهم وأسرع السير تسبق الأخبار، فإن أظفرك الله، فأقلل اللبث فيهم وخذ معك الأدلاء وقدم العيون أمامك والطلائع 381
- يأتي على الناس زمان لا يبالي المرء بما أخذ المال بحلال أو حرام 401

فهرس الجداول

رقم الجدول	بيـــــانـــــه	الصفحـــة
1	يبين مستعملي الانترنت في الدول الناطقة باللغة العربية (تقدير 31 ديسمبر 2011)	95
2	يبين حجم سرقة البرامج بالنسب المئوية في دول الشرق الأوسط والدول الإفريقية من سنة 2004 إلى غاية 2008	105
3	يبين مداخيل صناعة المواد الإباحية خلال سنة 2004	157

فهرس الأشكال والبيانات

رقم الشكل	بيـــــانـــــه	الصفحـــة
1	يوضح أنواع البرمجيات وعلاقاتها	49
2	يبين شبكة آربانت البحثية على الخريطة عام 1969م	53
3	يوضح المراحل التاريخية لتطور شبكة الانترنت	54
4	رسم بياني يمثل نسبة انتشار الانترنت بحسب المنطقة	88
5	رسم بياني يبين نسب الاختراقات الإلكترونية الحاصلة حسب المنطقة خلال سنة 2012	88
6	رسم بياني يبين حصة المتصفحات الرئيسية بالنسب المئوية حتى ديسمبر عام 2012	91
7	يبين أكثر اللغات استعمالا على الانترنت	93
8	يبين الدول العشر المصنفة الأكثر استعمالا للانترنت بالنسبة للدول الناطقة باللغة العربية	94
9	يبين عدد مستخدمي الانترنت لكل مائة ساكن عبر السنوات	96
10	يبين النسب المئوية لسرقة البرامج حسب مناطق العالم خلال سنتي: 2007 و 2008	106
11	يمثل عملية تفعيل الفيروس الملحق بالملف مباشرة أثناء تشغيل البرنامج	111
12	يبين طريقة انتشار فيروس الدودة بالنسبة للأجهزة التي لم تفعل وسائل الحماية الأمنية أو لم تحيّنها	113
13	يبين طريقة انتشار فيروس حصان طروادة ونشاطه	114
14	يمثل رسالة إلكترونية صدرت سنة 2006م تدعو عملاء بنك BNP Paribas لتحيين ملفاتهم، وحقيقتها أنها رسالة احتيالية لاصطياد المعلومات الخاصة بالعملاء	130
15	يظهر أحد مواقع المزاد الإلكتروني في دولة الإمارات العربية المتحدة	132
16	نموذج لأحد بطاقات الائتمان المتعامل بها وبياناتها	134
17	يبين أحد برامج التجسس المستعملة في الانترنت للحصول على كلمات المرور الخاصة بالبريد الإلكتروني	163
18	يبين الموقع الإلكتروني Silk Road لتجارة المخدرات بعد اكتشافه وتوقيفه	177
19	يظهر سوق افتراضية للأسلحة على موقع التواصل الاجتماعي الشهير "فايس بوك " يعرضها أحد الباعة الليبيين لعامة الناس، وقد بلغ عدد الذين أعجبهم الموقع في فترة وجيزة 10596 مطلّع	186
20	يبين طريقة عمل جدار الحماية	197

رقم الشكل	بيـــــانـــــه	الصفحـــة
21	يظهر الجدار الناري الموجه الحاجب Screening Router وهو يصل شبكة محلية بشبكات واسعة	198
22	يبين تحكم الوسيط Proxy في أمن المعلومات عبر الشبكة الداخلية وشبكة الانترنت	200
23	يوضح آلية التشفير المتماثل (Symmetric Cryptography)	203
24	يوضح آلية التشفير غير المتماثل (Asymmetric Cryptography)	204
25	يبين نافذة اختيارات للتوقيع الإلكتروني	211
26	يبين العناصر المكونة للحاسب الجنائي	216
27	يظهر نافذة أوامر برنامج البحث عن المفردات النصية String Search	217
28	يظهر نافذة عمل لبرنامج Extractor وهو يعمل على استرجاع الملفات الإلكترونية التي تم محوها من الحاسوب	218
29	يبين نافذة عمل لبرنامج Winhex	218
30	يبين نافذة أوامر لبرنامج Advanced PDF Password recovery Pro	219
31	يبين نافذة عمل لبرنامج VisualRoute وهو يقوم بتقفي الأثر	220
32	يوضح أهم المرفقات الخبيثة ونسبها في رسائل البريد الإلكتروني	362
33	يبين الصور الناتجة عن المسح المغناطيسي للمنطقة المسؤولة عن المكافأة في الدماغ حيث يظهر عليها نشاط غير عادي أثناء رؤية المشاهد الإباحية، وهو ما يفسر أن تكرار هذه المشاهد يؤثر على الدماغ وينهكه تماماً بنفس تأثير الإدمان على المخدرات والخمر حسب الدراسة	372
34	يوضح مسار ومهام مادتي Dopamine ، وSerotonin في دماغ الإنسان	373

فهرس المصادر والمراجع

القرآن الكريم.

﴿ أ ﴾

- ابن الأثير، أبو الحسن علي بن محمد بن عبد الكريم بن عبد الواحد الشيباني، الكامل في التاريخ، دار صادر للطباعة والنشر، بيروت، 1385هـ ـ1965م.
- ابن الجوزي؛ أبو الفرج جمال الدين عبد الرحمن، زاد المسير في علم التفسير، المكتب الإسلامي، بيروت، ط3، 1404هـ ـ 1984م.
- ابن القيم، الإمام العلامة شمس الدين أبو عبد الله محمد بن أبي بكر ابن القيم الجوزية، إعلام الموقعين عن رب العالمين، تحقيق طه عبد الرؤوف سعد، دار الطباعة المنيرية، القاهرة، دار الحديث، بيروت، 1973م.
- ابن القيم، الطرق الحكمية في السياسة الشرعية، تحقيق سيد عمران، دار الحديث، القاهرة، ط1، 2002م.
- ابن قيم الجوزية، محمد بن أبي بكر أيوب، زاد المعاد في هدي خير العباد، تحقيق شعيب الأرنؤوط وعبد القادر الأرنؤوط، ط3، مؤسسة الرسالة، بيروت، 1402هـ
- ابن قيم الجوزية، الطرق الحكمية في السياسة الشرعية، تحقيق الشيخ زكريا عميرات، دار الكتب العلمية، بيروت، 1996م.
- ابن قيم الجوزية، أعلام الموقعين عن رب العالمين، تحقيق محمد المعتصم بالله البغدادي، ط1، دار الكتاب العربي للطباعة والنشر والتوزيع.
- ابن العربي، أبو بكر ابن العربي المعافري المالكي، المحصول في أصول الفقه، تحقيق علي وسعيد فودة، ط1، دار البيارق، عمان، 1420هـ.
- ابن العربي المالكي، أحكام القرآن، تحقيق محمد القادر عطا، دار الكتب العلمية، بيروت.
- ابن الهمام، محمد بن عبد الواحد المعروف بابن الهمام، فتح القدير، دار الفكر، الطبعة الثانية، 1397هـ.
- ابن الهمام، شرح فتح القدير مع تكملة نتائج الأفكار في كشف الرموز والأسرار على الهداية، ط1، المطبعة الأميرية.
- ابن تيمية، أحمد عبد الحليم بن تيمية الحراني أبو العباس، كتب ورسائل وفتاوى ابن تيمية في الفقه، تحقيق عبد الرحمن محمد بن قاسم العاصمي النجدي، ط2، مكتبة ابن تيمية.
- ابن تيمية، الفتاوى الكبرى، تحقيق محمد عبد القادر عطا، ومصطفى عطا، دار الكتب العلمية.

- ابن تيمية، الاختيارات العلمية في اختيارات ابن تيمية ، مطبعة كردستان العلمية، مصر، 1329هـ.
- ابن تيمية؛ تقي الدين أبو العباس أحمد بن عبد الحليم: مجموع الفتاوى، مطبعة الحكومة، مكة المكرمة، السعودية، د.ط. 1389هـ ـ 1969م.
- ابن جزي، القوانين الفقهية، دار ابن حزم، طبعة 2013م.
- ابن حجر العسقلاني؛ أبو الفضل شهاب الدين أحمد بن علي: الإصابة، تحقيق علي محمد البجاوي، دار الجيل، بيروت، ط1، 1412هـ 1992م.
- ابن حجر العسقلاني؛ أبو الفضل شهاب الدين أحمد بن علي: العجاب في بيان الأسباب، تحقيق عبد الحكيم محمد الأنيس، دار ابن الجوزي ـ الدمام ـ السعودية، ط1، 1997م.
- ابن حجر العسقلاني؛ أبو الفضل شهاب الدين أحمد بن علي: فتح الباري شرح صحيح البخاري، ت: محمد فؤاد عبد الباقي ومحب الدين الخطيب، دار المعرفة ـ بيروت، لبنان، د.ط. 1379هـ.
- ابن حزم، أبو محمد علي بن أحمد بن سعيد الأندلسي، المحلى بالآثار، تحقيق الدكتور عبد الغفار سليمان البنداري، دار الكتب العلمية، بيروت.
- ابن حزم، الإحكام في أصول الأحكام، دار الآفاق الجديدة، 1983م.
- ابن حميد، حماية الحقوق الفكرية من منظور إسلامي، سجل الملتقى العلمي حول حماية الحقوق الفكرية، الكلية التقنية بالرياض، 1420هـ..
- ابن حنبل؛ الإمام أحمد الشيباني: مسند أحمد، دار صادر، بيروت، لبنان. د.ت.
- ابن رجب الحنبلي؛ أبو الفرج عبد الرحمن بن أحمد: جامع العلوم والحكم، دار المعرفة، ط1، 1408هـ.
- ابن رشد القرطبي، بداية المجتهد ونهاية المقتصد، دار الكتب العلمية، بيروت، 1408هـ ـ 1988م .
- ابن عابدين، حاشية ابن عابدين، دار إحياء التراث العربي، بيروت، 1972م،
- ابن عابدين، حاشية رد المحتار على الدر المختار، دار الفكر، بيروت، ط2، 1386هـ.
- ابن عابدين، رد المحتار على الدر المختار شرح تنوير الأبصار، دار الكتب العلمية، بيروت، لبنان، ط1، 1415هـ.
- ابن عاشور؛ محمد الطاهر: تفسير التحرير والتنوير، الدار التونسية للنشر ـ تونس ـ 1984م.
- ابن عباد إسماعيل، المحيط في اللغة، تحقيق الشيخ محمد حسن آل ياسين، ط1، بيروت، دار الكتب العلمية، 1414هـ.
- ابن عبد البر المالكي، الكافي في فقه أهل المدينة، ج1، مطبعة مكتبة الرياض الحديثة، الرياض، 1398هـ ـ 1978م.
- ابن عساكر الشافعي (ت: 571هـ)، تهذيب تاريخ دمشق الكبير، ترتيب عبد القادر بدران (ت: 1346هـ)، دار المسيرة، بيروت، لبنان، 1399هـ ـ 1979م.

- ابن فارس، أبو الحسن أحمد بن فارس بن زكريا، معجم مقاييس اللغة، تحقيق عبد السلام محمد هارون، ط2، دار الجيل، بيروت، لبنان، 1420هـ.
- ابن فرحون، برهان الدين أبي الوفاء إبراهيم بن الإمام شمس الدين أبي عبد الله محمد بن فرحون، تبصرة الحكام في أصول الأقضية ومناهج الأحكام، دار الكتب العلمية، بيروت، لبنان، 1422هـ.
- ابن قدامة، أبو محمد موفق الدين عبد الله بن قدامة المقدسي، ت 630هـ، المغني، تحقيق عبد الله بن عبد المحسن التركي، وعبد الفتاح محمد الحلو، دار هاجر للطباعة والنشر، القاهرة، ط2، 1413هـ.
- ابن قدامة، الكافي، تحقيق عبد الله بن عبد المحسن التركي، وعبد الفتاح محمد الحلو، دار هاجر، ط1، 1417هـ.
- ابن قدامة، المغني والشرح الكبير، تحقيق شمس الدين المقدسي، دار الكتب العلمية، بيروت، 1994م.
- ابن قدامة، روضة الناظر وجنة المناظر في أصول الفقه، مكتبة المعارف، الرياض.
- ابن قدامة المقدسي، المغني على مختصر الخرقي، ط1، دار الكتب العلمية، بيروت، 1414هـ ـ 1994م
- ابن كثير، أبو الفدا إسماعيل بن عمر بن كثير الدمشقي، تفسير القرآن العظيم المسمى بـ (تفسير ابن كثير)، بيروت، دار الفكر، 1401هـ.
- ابن ماجه، أبو عبد الله محمد بن يزيد القزويني، ت 273هـ، سنن ابن ماجه، تحقيق محمد فؤاد عبد الباقي، دار الفكر، بيروت، د.ت.
- ابن منظور، العلامة جمال الدين محمد بن مكرم بن منظور المصري، 630هـ ـ 711هـ، لسان العرب، ط1، دار صادر، بيروت، لبنان، 1990م.
- ابن نجيم، زيد الدين إبراهيم محمد بن بكر ابن نجيم، البحر الرائق شرح كنز الدقائق، دار المعرفة، بيروت، لبنان.
- ابن هشام، الإمام أبو محمد بن عبد المطلب بن هشام المعافري (ت: 218هـ)، السيرة النبوية، ط2، مطبعة الحلبي، 1375 هـ ـ 1955م،
- ابن هشام؛ أبو محمد عبد الملك بن أيوب الحميري: السيرة النبوية، تحقيق مصطفى السقا وآخرون، دار إحياء التراث العربي، بيروت، د.م.

- أبو الحسين أحمد بن فارس بن زكريا، معجم مقاييس اللغة، تحقيق عبد السلام محمد هارون، دار الجيل، بيروت، لبنان، 1999م.
- أبو الفدى إسماعيل بن عمر بن كثير الدمشقي، (ت: 744هـ): تفسير ابن كثير، ج4، بيروت، دار الفكر، 1401هـ.
- أبو الفضل العراقي، المغني عن حمل الأسفار في الأسفار، تحقيق أشرف عبد المقصود، ط1، مكتبة طبرية، الرياض، 1415هـ

- أبو الليل إبراهيم الدسوقي، الجوانب القانونية للتعاملات الإلكترونية، الكويت، جامعة الكويت، 2003م.
- أبو بكر بن حسن الكنشاوي، أسهل المدارك شرح إرشاد السالك في فقه إمام الأئمة مالك، ط2، مطبعة عيسى البابي الحلبي وشركاه، دمشق.
- أبو بكر جابر الجزائري، أيسر التفاسير لكلام العلي الكبير، دار السلام للطباعة والنشر، القاهرة، ط4، 1412هـ ـــ 1992م.
- أبو بكر محمد بن عبد الله بن العربي، أحكام القرآن، مطبعة عيسى البابي، مصر .
- أبو جعفر، محمد بن جرير بن يزيد خالد الطبري (224 310هـ)، جامع البيان عن تأويل آي القرآن المعروف بتفسير الطبري، دار الفكر، بيروت، 1405 هـ.
- أبو حامد العزالي، المستصفى من علم الأصول، شركة المدينة المنورة للطباعة، السعودية، 1356هـ.
- أبو حامد الغزالي، الوسيط في المذهب، تحقيق أحمد محمود إبراهيم، محمد محمد تامر، ط1، القاهرة، دار السلام، 1417هـ.
- أبو حامد الغزالي، إحياء علوم الدين، ط1، دار الكتب العلمية، بيروت، 1995م.
- أبو حامد الغزالي، المنخول في تعليقات الأصول، تحقيق حسن محمد هيتو،ط2، دار الفكر، دمشق، 1400هـ.
- أبو داود؛ سليمان بن الأشعث السجستاني: سنن أبو داود، مراجعة محمد الدين عبد الحميد، دار الفكر، د.م.
- أبو عبد الله محمد بن علي بن عمر المازري، (ت 536هـ ـــ 1141م)، المعلم بفوائد مسلم، تحقيق محمد الشاذلي النيفر، بيت الحكمة في الجزائر والمطبعة العربية في تونس، 1988.
- أبو عمرو عثمان بن سعيد المقرئ الداني، السنن الواردة في الفتن، ط2، تحقيق المباركفوري، دار العاصمة، الرياض، 1416هـ.
- أبو محمد علي بن أحمد بن حزم الأندلسي(ت 456هـ)، مراتب الإجماع، مطبعة المنيرية، القاهرة، 1350هـ.
- أبو محمد علي بن أحمد بن حزم الظاهري، المحلى، تحقيق أحمد محمد شاكر، دار التراث، القاهرة .
- أبو منصور محمد بن أحمد الأزهري، تهذيب اللغة، الدار المصرية للتأليف والترجمة، مصر.
- أبو نصر إسماعيل بن حماد الجوهري الفارابي، الصحاح تاج اللغة وصحاح العربية، ط4، دار العلم، بيروت
- أبو نعيم أحمد بن عبد الله الأصبهاني، حلية الأولياء ، دار الفكر العربي، بيروت، 1405هـ.
- أبو يوسف يعقوب بن إبراهيم، الخراج، ط3، المطبعة السلفية، القاهرة، 1382 هـ، ص 162، .
- أبي الحسن الماوردي، الأحكام السلطانية، دار الفكر للطباعة والنشر والتوزيع، لبنان، 1417 هـ، ص 219 .
- أبي عبد الله عليش، منح الجليل شرح مختصر خليل، ط1، دار الفكر، بيروت.
- أحمد إبراهيم سيد، التزوير المادي والمعنوي، دار الفكر الجامعي، 2003م.
- أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، جامعة نايف العربية للعلوم الأمنية، الرياض، 1414هـ.

- أحمد الحصري، السياسة الجنائية ، ط1، دار الجيل، 1992م.
- أحمد الريسوني، نظرية المقاصد عند الإمام الشاطبي، ط2، الدار العالمية للكتاب الإسلامي، الرياض، 1412 هـ ـ 1992م .
- أحمد السنهوري، الوسيط في شرح قانون العقوبات المدني التي تقع على الملكية والبيع والمقايضة، مطابع دار النشر للجامعات المصرية، 1996.
- أحمد الشرباصي، المعجم الاقتصادي الإسلامي، دار الجيل، 1971 .
- أحمد الفيومي، المصباح المنير، مطبعة الأميرية، القاهرة 1962م.
- أحمد المزغني، التشريعات الجنائية ومكافحة الجريمة، المركز العربي للدراسات الأمنية، الرياض، 1408هـ.
- أحمد بن محمد الزرقاء، شرح القواعد الفقهية، ط2، تصحيح وتعليق مصطفى ابن المؤلف، دار القلم، دمشق، 1357هـ ـ 1938م.
- أحمد بن محمد بن حنبل، مسند الإمام أحمد، دار إحياء التراث العربي، بيروت، 1414هـ ـ 1993م.
- أحمد بن محمد بن علي المقري الفيومي، المصباح المنير في غريب الشرح الكبير للرافعي، دار الكتب العلمية، بيروت، لبنان، 1994م.
- أحمد حسام تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2000م.
- أحمد حسن، الأوراق النقدية في الاقتصاد الإسلامي، دار الفكر، دمشق، 2002م.
- أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الاسكندرية، 2006م.
- أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية 2006م.
- أحمد زكي بدوي، معجم مصطلحات العلوم الاجتماعية، مكتبة لبنان، بيروت، 1986.
- أحمد عبد العزيز الألفي، شرح قانون العقوبات القسم العام مكتبة النصر، الزقازيق، مصر، 1995م.
- أحمد عوض بلال، محاضرات في الجزاء الجنائي، درا النهضة العربية، القاهرة، 2002م.
- أحمد فتحي بهنسي، السياسة الجنائية في الشريعة الإسلامية، ط1، دار الشروق، 1403هـ ـ 1983م.
- أحمد فتحي بهنسي، مدخل الفقه الجنائي الإسلامي، دار الشروق، القاهرة، مصر، 1409هـ ـ 1989م.
- أحمد فتحي سرور، الوسيط في قانون العقوبات القسم العام ـ، ط6، دار النهضة العربية، القاهرة، 1996.
- أحمد محمود خليل، جرائم تزوير المحررات، المكتب الجامعي الحديث، الإسكندرية، دار الفكر الجامعي،2008م.
- أحمد هابي، الجاسوسية بين الوقاية والعلاج، الشركة المتحدة للنشر والتوزيع، القاهرة، 1974م.
- أروى فايز الفاعوري وإناس محمد قطيشات، جريمة غسيل الأموال العامة والطبيعة القانونية، دار وائل للنشر، الطبعة الأولى، 2002.
- الأزهري، أبو منصور محمد بن أحمد، تهذيب اللغة، تحقيق محمد عوض مرعب، ط1، بيروت، دار إحياء التراث العربي، 2001م.

- أسامة أحمد المناعسة، جلال محمد ، صايل فاضل الهواوشة، جرائم الحاسب الآلي والإنترنت، دار وائل للطباعة والنشر، ط1، 2001م.
- أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، دراسة مقارنة، دار النهضة العربية، 2005.
- اسماعيل بن حماد الجوهري، الصحاح، دار العلم للملايين، بيروت، ط3، 1990م، ص 448 .
- إسماعيل بن عباد، المحيط في اللغة، تحقيق: الشيخ محمد حسن آل ياسين، ط1، دار الكتب العملية، بيروت، 1414هـ.
- إسماعيل محمد رشدي، الجنايات في الشريعة الإسلامية، دار الأنصار، القاهرة، 1983م .
- الإسنوي، التمهيد في تخريج الفروع على الأصول، تحقيق محمد حسن هيتو، الرسالة، بيروت ط1، 1400هـ.
- أشرف توفيق شمس الدين، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية 2007 .
- الألوسي؛ أبو الفضل شهاب الدين: روح المعاني في تفسير القرآن العظيم والسبع المثاني، دار إحياء التراب العربي، بيروت، لبنان، د.م.
- آمال عبد الرحيم عثمان،الإثبات الجنائي ووسائل التحقيق العلمية، دار النهضة العربية، القاهرة، 1975م.
- الإمام أحمد بن حنبل، مسند الإمام أحمد بن حنبل، مجموعة من المحققين، بإشراف الدكتور: عبد الله بن عبد المحسن التركي، مؤسسة الرسالة، بيروت، لبنان، ط1، 1416هـ.
- إمام حسنين، جرائم الإرهاب الدولي في التشريعات المقارنة، دار المطبوعات الجامعية، مصر، 2012م.
- الإمام مالك، أبو عبد الله مالك ابن أنس بن مالك بن أبي عامر بن عمرو بن الحارث، ت 179هـ، الموطأ، تحقيق محمد فؤاد عبد الباقي، دار إحياء التراث العربي، بيروت.
- الإمام مالك: موطأ مالك، رواية يحي بن يحي الليثي، إعداد أحمد راتب عرموش، دار النفائس، بيروت، ط11، 1410هـ ـــ 1990م.
- أمجد حمدان الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، ط1، دار المسيرة، عمان، الأردن، 2010.
- الآمدي، الإحكام في أصول الأحكام، تحقيق سيد الجميلي، ط1، دار الكتاب العربي، بيروت، 1404هـ .
- أمين مصطفى محمد، مبادئ علم الإجرام، دار الجامعة الجديدة، الإسكندرية، 1996م.
- إيهاب فوزي السقا، الحماية الجنائية لبطاقات الائتمان، دار الجامعة الجديدة، الاسكندرية 2008.

﴿ ب ﴾

- البجيرمي سليمان بن محمد بن عمر(1221هـ)، نهاية المحتاج إلى شرح المنهاج، مطبعة الحلبي، القاهرة، 1358هـ.
- البخاري، أبو عبد الله بن إسماعيل البخاري، صحيح البخاري، دار الدعوة، اسطنبول، ودار سحنون، تونس، ط2، 1413هـ.
- البخاري؛ أبو عبد الله محمد بن إسماعيل بن إبراهيم الجعفي: الجامع الصحيح، مراجعة د. مصطفى ديب البغا، دار ابن كثير، اليمامة، بيروت، د.ط. 1407هـ ـ 1987م.
- البزدوي، علي بن محمد الحنفي، كتر الوصول إلى معرفة الأصول المعروفة بأصول البزدوي، مطبعة جاويدبريس، كراتشي.
- بطرس البستاني، محيط المحيط، مكتبة لبنان، بيروت، 1987م.
- البغوي؛ أبو محمد الحسين بن مسعود الفراء: معالم التنزيل، تحقيق خالد العك ومروان سوار، دار المعرفة ـ بيروت، ط2، 1407هـ ـ 1987م.
- البغوي، شرح السنة، ط1، تحقيق شعيب الأرناؤوط، المكتب الإسلامي، بيروت، 1403هـ ـ 1983م.
- بكر بن عبد الله أبو زيد، فقه النوازل، مؤسسة الرسالة، ط1، 1416هـ.
- البلاذري، فتوح البلدان، دار الفكر، بيروت، ط1، 1992.
- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، الاسكندرية، مصر، 2008م.
- بهاء الدين الشامي، تحديات أمن المعلومات، دار العلوم للنشر والتوزيع والطباعة، حلب، سوريا، 2007. .
- البهنسي؛ أحمد فتحي: مدخل الفقه الجنائي الإسلامي، دار الشروق، ط4، القاهرة، 1403هـ ـ 1983م.
- البهنسي؛ أحمد فتحي: نظرية الإثبات في الفقه الجنائي الإسلامي، دار الشروق، ط5، القاهرة، 1403هـ ـ 1983م.
- البهوتي: الروض المربع شرح زاد المستنقع في اختصار المقنع، تحقيق سعيد محمد اللحام، دار الفكر للطباعة والنشر، بيروت، لبنان.
- بوساق؛ محمد بن المدني: اتجاهات السياسة الجنائية المعاصرة والشريعة الإسلامي، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، 1423هـ ـ 2002م.
- البوطي، حق الإبداع، قضايا فقهية معاصرة، مكتبة الفارابي، دمشق، ط1، 1419هـ ـ 1999م
- البيهقي، أحمد بن الحسين بن علي أبو بكر ت 458هـ، كتاب السنن الكبرى، ط1413هـ ـ 1992م، دار المعرفة، بيروت.

- البيهقي؛ أبو بكر أحمد بن الحسين: السنن الكبرى، تحقيق محمد عبد القادر عطا، مكتبة دار الباز، مكة المكرمة، ط1، 1414هـ ـ 1994م.
- البيهقي؛ أبو بكر أحمد بن الحسين: شعب الإيمان، تحقيق محمد السعيد بسيوني زغلول، دار الكتب العلمية، بيروت، ط1، 1410هـ.

﴿ ت ﴾

- الترمذي، أبو عيسى بن عيسى بن سورة الترمذي، ت 279هـ ، سنن الترمذي، ط2، دار الدعوة اسطنبول، ودار سحنون، تونس، 1413هـ.
- الترمذي، سنن الترمذي، أو المسمى الجامع الصحيح، تحقيق محمد فؤاد عبد الباقي، دار الكتب العلمية، بيروت.
- التفتزاني، شرح التلويح على التوضيح في أصول الفقه، مطبعة صبيح، القاهرة، 1377هـ ـ 1957م
- التلمساني، المالكي، مفتاح الوصول إلى بناء الفروع على الأصول، المطبعة الأهلية، تونس، 1346هـ.

﴿ ث ﴾

- ثروت عبد الحميد، التوقيع الإلكتروني، ماهيته مخاطره، وكيفية مواجهتها، مدى حجيته في الإثبات، مكتبة الجلاء الجديدة بالمنصورة، 2001.

﴿ ج ﴾

- الجرجاني، التعريفات، تحقيق إبراهيم البياري، دار الكتاب العربي، بيروت، ط1، 1405هـ.
- الجصاص، أحمد بن علي أبو بكر الرازي، ت 370هـ ، أحكام القرآن ، دار الكتب العلمية، بيروت، 1400هـ.
- الجصاص، أحكام القرآن، تحقيق محمد الصادق قمحاوي، ط2، دار المصحف، القاهرة.
- جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية،القاهرة، 2001م.
- جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية، القاهرة 1999م.

- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة ـــ الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992م.

﴿ ح ﴾

- الحافظ أبو داود سليمان بن الأشعث، سنن أبي داود، دار الدعوة، اسطنبول، ودار سحنون، تونس، ط2، 1413هـ.
- الحجاوي، الإقناع لطالب الانتفاع، ط2، دار عالم الكتب، الرياض، 1419هـ ـــ 1999م.
- حسام العبد، مكافحة غسيل الأموال في البنوك والمؤسسات المالية، معهد الدراسات المصرفية، عمان، 2003.
- حسام شوقي، حماية المعلومات على الانترنت، دار الكتب العلمية، القاهرة، 2003م .
- حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، القاهرة، 1987م.
- حسن سعيد الكرمي، المغني الأكبر (انجليزي عربي)، مكتبة لبنان، 1987م.
- حسن صادق المرصفاوي، الإجرام والعقاب في مصر، منشأة المعارف، الإسكندرية، 1973م.
- حسن طاهر داود، الحاسب وأمن المعلومات، معهد الإدارة العامة ، الرياض، 2000م.
- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1420هـ.
- حسين محمد الربابعة، أحكام الشهادة وعقوبة شاهد الزور في الإسلام، ط1، دار يافا العلمية، 2007م.
- الحطاب، محمد بن محمد، مواهب الجليل، ط1، دار الكتب العلمية، بيروت، 1990م.
- الحطاب، الأشباه والنظائر، دار الكتب العلمية، بيروت، 1405هـ.
- حمدان القاضي، جرائم الانترنت، دار الفكر ، بيروت، 2007م.
- الحمدان عبد الرحمن القاسم، أساسيات أمن المعلومات، مكتبة فهد الوطنية، ط2، 2008 ..
- حمدي عبد العظيم، غسيل الأموال في مصر والعالم، الدار الجامعية للطباعة والنشر والتوزيع، 2007م.
- الحموي، أحمد بن محمد: غمز عيون البصائر شرح الأشباه والنظائر، ط1، دار الطباعة، القاهرة.

﴿ خ ﴾

- خالد الطويل و عبد الرحمن العلي و نزال مبروكة، مدخل إلى الإنترنيت وتكنولوجيا الحاسب الشخصي، ط1، الدار العربية للعلوم، بيروت 1420هـ.

- خالد بن سليمان الغثبر، وزياد بن عثمان الحقيل، الاصطياد الإلكتروني الأساليب والإجراءات المضادة، مكتبة فهد الوطنية، الرياض، ط1، 2009م.
- خالد محمود عبد الغني، رحلة إلى عالم الانترنيت، مركز تطوير البرمجيات المقترحة، القاهرة، مصر، 1997م.
- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2009م .
- خالد ممدوح إبراهيم، أمن مراسلات البريد الإلكتروني، الدار الجامعية، مصر، 2011م.
- الخطيب الشربيني، مغني المحتاج إلى معرفة شرح معاني المنهاج، دار الكتب العلمية، بيروت.
- الخليل الفراهيدي، كتاب العين، المكتبة الوطنية، بغداد، 1982م. .
- خير الدين حسين محمد، الأصول العلمية للإعلان، مكتبة عين شمس، القاهرة، ط 1982.
- خير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، 2010.

﴿ د ﴾

- الدارقطني؛ أبو الحسن علي بن عمر: سنن الدارقطني، تحقيق السيد عبد الله هاشم يماني المدين، دار المعرفة، بيروت، ط1386هـ ـ 1966م.
- الدارمي، عبد الله بن عبد الرحمن بن الفضل، ت255هـ، سنن الدارمي، دار الدعوة، اسطنبول، ودار سحنون، تونس، ط2، 1413هـ.
- داود حسن طاهر، الحاسب وأمن المعلومات، الرياض، معهد الإدارة العامة، 2000م.
- الدردير، الشرح الكبير ومعه حاشية الدسوقي، المطبعة الأميرية.
- الدسوقي، شمس الدين محمد بن عرفة الدسوقي، حاشية الدسوقي، على الشرح الكبير، دار الفكر، بيروت.

﴿ ر ﴾

- الرازي، فخر الدين محمد بن عمر التميمي الرازي الشافعي، مفاتح الغيب المسمى بـ (التفسير الكبير)، ط1، دار الكتب العلمية، بيروت، 1421هـ.
- الرازي، مختار الصحاح، تحقيق محمود خاطر، مكتبة لبنان، بيروت، 1415هـ ـ 1995م.
- راشد علي، القانون الجنائي المدخل وأصول النظرية العامة، ط2، دار النهضة العربية، القاهرة، 1974م.
- الراغب الأصفهاني؛ أبو القاسم الحسين بن محمد بن الفضل: معجم مفردات ألفاظ القرآن الكريم، ضبط وتخريج وتصحيح: ابراهيم شمس الدين ، منشورات محمد علي بيضون، دار الكتب العلمية، بيروت، ط1، 1418هـ ـ 1997م.

- رأفت نبيل علوة، قرصنة الانترنت، مكتب المجتمع العربي، الأردن، ط1، 2006م.
- رحيمة الصغير ساعد نمديلي، العقد الإداري الإلكتروني، دراسة تحليلية مقارنة، دار الجامعة الجديدة 2007م.
- رضا محمد، معجم متن اللغة، دار مكتبة الحياة، بيروت، 1977.
- رمزي نجيب القسوس، غسيل الأموال جريمة العصر، دار وائل للنشر، عمان، الأردن، 2002م.
- رمسيس بهنام، المجرم تكوينا وتقويما، منشأة المعارف، الإسكندرية 1995.
- رمضان السيد، الجريمة والانحراف من المنظور الاجتماعي، المكتب الجامعي الحديث، الاسكندرية،1985.
- رؤوف عبيد، مبادئ القسم العام من التشريع العقابي، دار الفكر العربي، بيروت، 1979م، ص 19.
- رؤوف عبيد، مبادئ القسم العام من التشريع العقابي، ط3، دار الفكر العربي، القاهرة، 1966م.
- رياض فتح الله بصيلة، جرائم بطاقات الائتمان دراسة معرفية تحليلية لمكوناتها وأساليب تزييفها وطرق التعرف عليها ـــ، ط1، دار الشروق، القاهرة، 1995م.

﴿ ز ﴾

- الزبيدي، أبو الفياض محمد ابن محمد عبد الرزاق الحسيني، تاج العروس من جواهر القاموس، تحقيق مجموعة من الحققين، دار صادر، بيروت، 1386هـ ـــ 1966م.
- الزحيلي؛ د. وهبة: التفسير المنير في العقيدة والشريعة والمنهج، دار الفكر، بيروت/دمشق، ط1، 1411هـ ـــ 1991م.
- الزحيلي؛ د. وهبة: الفقه الإسلامي وأدلته، دار الفكر ـــ دمشق، سوريا، ط3، 1409هـ ـــ 1989م.
- الزرقاني، شرح الزرقاني على موطأ الإمام مالك، دار الكتب العلمية، 1993م.
- الزرقاني؛ محمد عبد العظيم: مناهل العرفان في علوم القرآن، دار الفكر ـــ بيروت، ط1، 1996م.
- الزركشي، بد الدين محمد بن بهادر بن عبد الله، ت 794هـ، شرح الزركشي على مختصر الخرقي، دار الكتب العلمية، 2002م.
- زكي الدين شعبان، أصول الفقه، دار الكتب والوثائق العراقية، بغداد، 1983م
- الزمخشري، الكشاف عن حقائق التنزيل وعيون الأقاويل في وجوه التأويل، تحقيق عبد الرزاق المهدي، دار إحياء التراث العربي، بيروت. .
- الزمخشري؛ أبو القاسم جارالله: الكشاف عن حقائق التنزيل وعيون الأقاويل في وجوه التأويل، دار الفكر، ط1، 1397هـ ، 1977م.
- الزمخشري، المصباح المنير، تحقيق محمد أحمد قاسم، أحمد حمصي، المكتبة العصرية، بيروت.

- زهرة محمد مرسي، الحاسوب والقانون، مؤسسة الكويت للتقدم العلمي، الكويت، 1995م.
- زيد المدخلي، الإرهاب وآثاره على الأفراد والأمم، دار المنهاج، الرياض،1417هـ.
- الزيلعي، جمال الدين محمد بن عبد الله الزيلعي، نصب الراية تخريج أحاديث الهداية، تحقيق أحمد شمس الدين، ط1، دار الكتب العلمية، بيروت، 1990م.
- الزيلعي، حاشية شهاب الدين على شرح الكنز، دار المعرفة للطباعة والنشر، بيروت، 1313هـ.

﴿ س ﴾

- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الاسكندرية، 2007.
- السبكي؛ تاج الدين عبد الوهاب بن علي: الأشباه والنظائر، ت: عادل أحمد عبد الموجود وعلي محمد عوض، دار الكتب العلمية، بيروت، لبنان، ط1، 1411هـ ـ 1991م.
- السبكي، طبقات الشافعية الكبرى، تحقيق مصطفى عبد القادر عطا، ط1، دار الكتب العلمية، بيروت.
- سرحان سليمان داود، محمود عبد المنعم المشهداني، أمن الحاسوب والمعلومات، دار وائل، عمان، الأردن، 2001م.
- السرخسي، شمس الدين أبو بكر محمد السرخسي، المبسوط، ط1، دار الفكر، بيروت.
- سعود عبد الله الحزيمي، الموسوعة الجامعة في الأخلاق والسلوك، دار الفجر، 2005.
- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت الجرائم الواقعة في مجال تكنولوجيا المعلومات ط1، دار النهضة العربية، القاهرة، 1999م.
- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية "الإنترنت"، دار النهضة العربية، القاهرة، 2007م.
- سليمان عبد المنعم، النظرية العامة لقانون العقوبات، منشورات الحلبي الحقوقية، بيروت، 2003.
- سمير الخطيب، مكافحة عمليات غسيل الأموال، منشأة المعارف، الإسكندرية، 2005.
- سهيل إدريس، قاموس المنهل (فرنسي عربي)، الطبعة الثالثة عشرة دار الآداب، بيروت، 1994م.
- سيد زكريا، عزت عبد القادر، محمد عبد المعز، جرائم التزييف والتزوير في ضوء الفقه والقضاء، دار الحقانية، مصر، 2004.
- السيد سابق، فقه السنة، ط4، دار الفكر للطباعة والنشر والتوزيع، بيروت، 1983م.
- السيوطي، جلال الدين عبد الرحمن بن أبي بكر، ت 911هـ، الأشباه والنظائر في قواعد وفروع فق الشافعية، ط1، دار الكتب العلمية، بيروت، 1990م.
- السيوطي؛ الدر المنثور في التفسير بالمأثور، دار الفكر ـ بيروت، د.ط.، 1993م.

﴿ ش ﴾

- الشاطبي، أبو إسحاق إبراهيم اللخمي الغرناطي، ت 790هـ، الموافقات.
- شريف سيد كامل، الجريمة المنظمة في القانون المقارن، دار النهضة العربية، القاهرة 2001م.
- شهاب الدين أحمد بن محمد بن سلامة قليوبي، حاشية قليوبي على شرح المحلى، شركة مكتبة ومطبعة مصطفى البابي الحلبي، مصر.
- شهاب الدين السيد محمود الألوسي البغدادي (ت:1270هـ)، روح المعاني في تفسير القرآن العظيم، دار إحياء التراث العربي، بيروت، لبنان.
- الشوكاني، محمد بن علي بن محمد، ت: 1255هـ، فتح القدير الجامع بين فني الرواية والدراية في علم التفسير، تحقيق سيد إبراهيم، دار زمزم، ط1، الرياض، د.ت.
- الشيخ محمد الطاهر بن عاشور، مقاصد الشريعة الإسلامية، دار النفائس للنشر والتوزيع، الأردن، ط2، 2001م.
- الشيرازي، إبراهيم بن علي الشيرازي، المهذب في فقه الإمام الشافعي، دار الفكر، بيروت، لبنان.
- الشيرازي، اللمع في أصول الفقه، مطبعة البابي الحلبي، مصر، 1358هـ ـــ 1939م.

﴿ ص ﴾

- الصابوني؛ محمد علي: قبس من نور القرآن الكريم، دراسات قرآنية، مكتبة رحاب، الجزائر، ط2، 1409هـ ـــ 1989م.
- صبحي فندي الكبيسي، علاقة علم الأصول بالمسائل الاقتصادية، بحث مقدم إلى مؤتمر علم أصول الفقه وصلته بالأصول الأخرى، كلية الشريعة، دبي، د.ت.
- صفي الرحمن المباركفوري، إبراز الحق والصواب في مسألة السفور والحجاب، ط2، دار الطحاوي، الرياض، 1417هـ.
- صلاح الدين السيسي، غسيل الأموال، قضايا اقتصادية معاصرة، مكتبة دار الآداب، الشارقة، 1998.
- الصنعاني، محمل بن إسماعيل الصنعاني، سبل السلام شرح بلوغ المرام، تخريج محمد عبد القادر عطا، دار الكتب العلمية، بيروت، لبنان، ط1، 1408هـ.

﴿ ط ﴾

- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.
- طارق الشهري، آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر والتوزيع، السعودية، 1421هـ.
- طارق بن عبد الله الشدي، مقدمة في الحاسب الآلي وتقنية المعلومات، ط2، دار الوطن للنشر ، الرياض.
- طارق عبد الله الشدي، آلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة والنشر والإعلام، الرياض، 2000م.
- الطاهر أحمد الزاوي: مختار القاموس، الدار العربية للكتاب، 1963م.
- طاهر مصطفى، المواجهة التشريعية لظاهرة غسل الأموال المتحصلة من جرائم المخدرات، التجهيزات الفنية والطباعة، القاهرة 2004م..
- الطائي يوسف، العبادي هشام، التسويق الإلكتروني، مؤسسة الوراق للنشر والتوزيع، الأردن، 2009م.
- الطبراني؛ أبو القاسم سليمان بن أحمد: المعجم الكبير، حمدي بن عبد المجيد، مكتبة العلوم والحكم، الموصل، ط2، 1404هـ ـ 1984م.
- الطبراني؛ أبو القاسم سليمان بن أحمد، المعجم الأوسط، ت: طارق بن عوض الله، دار الحرمين، القاهرة، مصر، د.ط. 1415هـ .
- الطبراني، المعجم الصغير، تحقيق محمد شكور محمد، ط1، المكتب الإسلامي، دار عمان، عمان، 1405هـ
- الطبري، محمد بن جرير، ت: 310هـ، جامع البيان في تفسير القرآن، دار الحديث، القاهرة، 1407هـ.
- الطبري؛ أبو يزيد محمد بن جرير: تفسير الطبري من كتابه جامع البيان عن تأويل آي القرآن، هذبه وحققه وضبط نصه وعلقه عليه: د. بشار عواد معروف وعصام فارس الحرساني، مؤسسة الرسالة ـ بيروت، ط1، 1415هـ ـ 1994م.
- الطبري؛ أبو يزيد محمد بن جرير: جامع البيان في تأويل آي القرآن، دار الكتب العلمية، بيروت، لبنان، ط2، 1412هـ ـ 1992م.

- الطحاوي، شرح معاني الآثار، ط1، عالم الكتب للطباعة والنشر والتوزيع، لبنان.
- الطوفي، شرح مختصر الروضة، مؤسسة الرسالة، 1987م.
- طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنيت، ط1، دار صادر، بيروت، لبنان، 2001 م.

﴿ ع ﴾

- عامر إبراهيم قنيلدجي، المعجم الموسوعي لتكنولوجيا المعلومات والإنترنت، المسيرة للنشر والتوزيع، 2010. .
- عامر السالمي، القانون الجنائي الخاص، مكتبة المعارف، المغرب، 1997م.
- عبد الحميد الشواربي: التزوير والتزييف مدنيا وجنائيا، منشأة المعارف، الإسكندرية.
- عبد الحميد بسيوني، التجارة الإلكترونية، دار الكتب العلمية للنشر والتوزيع، القاهرة، مصر، 2003.
- عبد الحميد ثروت، التوقيع الإلكتروني ماهيته ومدى حجيته في الإثبات، الإسكندرية، دار الجامعة الجديدة، ط2، 2008م.
- عبد الرحمان الهاشمي و فائزة محمد العزاوي، المنهج و الاقتصاد المعرفي ، دار المسيرة ، عمان ، الأردن ، ط1، 2007.
- عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات الانترنت دار الوراقين للنشر والتوزيع، بيروت، الطبعة الأولى، 2004.
- عبد الرحمن بن قاسم النجدي، مجموع فتاوى ابن تيمية، ط1، مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت.
- عبد الرحمن بن قدامة، الشرح الكبير، المجلد الخامس،ط1، هجر للطباعة والنشر، مصر، 1417هـ ـ 1996م.
- عبد الرحيم صدقي، الجريمة والعقوبة في الشريعة الإسلامية، ط1، مطبعة النهضة، مصر، 1408هـ.
- عبد الصبور عبد القوي، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، مصر، 2007م.
- عبد العزيز الزومان، شبكة الانترنيت، مدينة الملك عبد العزيز للعلوم والتقنية، وحدة خدمات الانترنيت، الرياض، 1422هـ.
- عبد العزيز بن أحمد المسعود، الأمر بالمعروف والنهي عن المنكر وأثرهما في حفظ الأمة، دار الحرمين للطباعة، القاهرة، ط1، 1415هـ.
- عبد العزيز عامر، التعزير في الشريعة الإسلامية، ط3، مطبعة مصطفى البابي الحلبي، مصر، 1957م.
- عبد الفتاح الصيفي، قانون العقوبات اللبناني جرائم الاعتداء على أمن الدولة وعلى الأموال دار النهضة العربية، بيروت 1972 .
- عبد الفتاح بيومي حجازي، الأحداث والانترنت، دار الفكر الجامعي، الإسكندرية، ط 2002.
- عبد الفتاح بيومي حجازي، الحماية الجنائية للتجارة الإليكترونية، المجلد الثاني، ط2، دار الكتب القانونية، 2008.
- عبد الفتاح بيومي حجازي، مقدمة في التجارة الإليكترونية العربية، المجلد الثاني، النظام القانوني للتجارة الإليكترونية في دولة الإمارات العربية المتحدة، دار الفكر الجامعي، الإسكندرية، 2004م.

- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، 2009م.
- عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، 2002، دار الكتب القانونية، القاهرة.
- عبد الفتاح حجازي، مقدمة في التجارة الإلكترونية العربية، الكتاب الأول: شرح قانون المبادلات والتجارة الإلكترونية التونسي، دار الفكر الجامعي، الاسكندرية، 2004م.
- عبد الفتاح مصطفى الصيفي،الأحكام العامة للنظام الجزائي في ضوء أنظمة المملكة العربية السعودية، جامعة الملك سعود 1407هـ.
- عبد القادر عودة، التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي، دار الكتاب العربي، بيروت، 1977.
- عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، دار الوراق، بيروت، 2004م.
- عبد الله العازي، شبكة الانترنت، دار القدس للعلوم، دمشق، سوريا، 2004م.
- عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011م .
- عبد الله بن عبد العزيز العجلان، القواعد الكبرى في الفقه الإسلامي، دار طيبة، الرياض، 1416هـ.
- عبد الله بن عبد العزيز اليوسف، الظواهر الإجرامية المستحدثة وسبل مواجهتها، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999م.
- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007 ، ص 42 43.
- عبد الله علي محمد، مكافحة جرائم الكمبيوتر والانترنت، الدار الجامعية للنشر، بيروت، 2007م.
- عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، ص 12 .
- عبد الوهاب خلاف، مصادر التشريع فيما لا نص فيه، طبعة معهد الدراسات العربية، 1954.
- عبود السراج: علم الإجرام وعلم العقاب، دراسة تحليلية في أسباب الجريمة وعلاج السلوك الإجرامي، ط2. دار السلاسل، الكويت، 1990م.
- عطا محمد السنباطي، موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت ، دار النهضة العربية ،ط1، 1422هـ.
- العظيم آبادي، محمد شمس الحق، عون المعبود شرح سنن أبي داود، دار الكتب العلمية، بيروت.
- العقيد صالح بن سعد الصالح، مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي، جامعة نايف العربية للعلوم الأمنية، 2008م ، الرياض
- عقيلي عمر، مبادئ التسويق، دار زهران، عمان، الأردن، ط1994م.

- علاء الدين الكاساني، بدائع الصنائع في ترتيب الشرائع، دار الكتاب العربي، بيروت، لبنان، ط2، 1402هـ.
- علاء السالمي، تكنولوجيا المعلومات، ط3، دار المناهج، عمان، الأردن، 2004م.
- علاء السالمي، شبكات الإدارة الإلكترونية، دار وائل للنشر، عمان، الأردن، 2003م.
- علاء السالمي، محاضرات مساق تكنولوجيا المعلومات، جامعة العلوم التطبيقية، 1997م.
- علاء عبد الرزاق محمد السالمي، نظم إدارة المعلومات، المنظمة العربية للتنمية الإدارية، ط1، 2003م، القاهرة.
- علال الفاسي، مقاصد الشريعة الإسلامية ومكارمها، ط5، دار المغرب الإسلامي، المغرب.
- علي السلمي، الإعلان، مكتبة شارع كامل صدقي، الفجالة، القاهرة، ب.س.ط.
- علي بن أبي بكر الهيثمي، مجمع الزوائد، دار الريان للتراث، دار الكتاب العربي، القاهرة، بيروت، 1407هـ.
- علي بن أحمد بن حزم، المحلى، المطبعة المنيرية، القاهرة، 1350هـ .
- علي حسن الشرفي، الباعث وأثره في المسؤولية الجنائية، الزهراء للإعلام العربي، 1986م.
- علي حسين الخلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت، 1982م.
- علي عبد القادر القهوجي، أصول علمي الإجرام والعقاب، منشورات الحلبي الحقوقية، 2002م.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، 1997.
- علي عبد القادر القهوجي، شرح قانون العقوبات القسم العام منشورات الحلبي الحقوقية، بيروت 2002.
- علي محمد جعفر، مكافحة الجريمة، الطبعة الأولى، المؤسسة الجامعية للدراسات والنشر، بيروت، 1998.
- عماد سلامة، الحماية القانونية لبرامج الحاسب الآلي، ط1، دار وائل للنشر، عمان، 2005م.
- عمر محمد بن يونس، المخدرات والمؤثرات العقلية عبر الإنترنت، دار الفكر الجامعي ، الإسكندرية 2004م.
- عوض محمد، مبادئ علم الإجرام وعلم العقاب، دار الجامعة الجديدة للنشر، الإسكندرية، 2000م.

﴿ غ ﴾

- الغزالي؛ محمد: نحو تفسير موضوعي لسور القرآن الكريم، دار الشروق، القاهرة، د.ط.، 1992م.
- غسان رباح، جريمة تبييض الأموال، دراسة مقارنة، المؤسسة الحديثة للكتاب، ط2، طرابلس، 2005.

﴿ ف ﴾

- فتاوى اللجنة الدائمة للبحوث العلمية والإفتاء، جمع وترتيب أحمد الدويش، طبع ونشر رئاسة البحوث العلمية والإفتاء الرياض،ط1، 1407هـ.
- فتحي الدريني، حق الابتكار في الفقه الإسلامي المقارن، ط3، مؤسسة الرسالة، بيروت، 1404هـ ـ 1984م.
- فتوح الشاذلي، أساسيات علم الإجرام والعقاب، منشورات الحلبي الحقوقية، بيروت، 2006م.
- فتوح الشاذلي، وعفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، بيروت، منشورات الحلبي الحقوقية، 2003م.
- فتوح عبد الله الشاذلي، شرح قانون العقوبات القسم العام ـ، دار المطبوعات الجامعية، الاسكندرية، مصر.
- فريد منعم جبور، حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010م.
- فهد بن عبد الرحمن الشميمري، التربية الإعلامية، مكتبة الملك فهد الوطنية،الرياض، 1431هـ ـ 2010م.
- فؤاد جمال، جرائم الحاسبات والإنترنت،الجرائم المعلوماتية، مركز المعلومات ودعم اتخاذ القرار، مصر، مارس 2005.
- فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية 1988.
- الفيروزآبادي، مجد الدين محمد بن يعقوب، القاموس المحيط، ط2، مؤسسة الرسالة، بيروت، 1407هـ.
- الفيروز آبادي؛ أبو طاهر بن يعقوب: تنوير المقابس في تفسير ابن عباس، مطبعة الأنوار المحمدية، القاهرة، د.م.
- الفيومي، أحمد بن محمد بن علي المقري، المصباح المنير في غريب الشرح الكبير للرافعي، المكتبة العلمية، بيروت، 1987م.

﴿ ق ﴾

- قاسم القونوي، أنيس الفقهاء في تعريفات الألفاظ المتداولة بين الفقهاء، تحقيق أحمد الكبيسي، دار الوفاء، ط1، 1406هـ.
- القرافي شهاب الدين أبو العباس، شرح تنقيح الفصول، دار الفكر، بيروت، لبنان، 1973م.
- القرافي، الذخيرة، تحقيق محمد حجي، بيروت، دار الغرب، 1994م.
- القرافي، الفروق، عالم الكتب، بيروت.

- القرطبي، أبو عبد الله أحمد بن أبي بكر بن فرج الأنصاري، ت 671هـ، تفسير القرطبي (الجامع لأحكام القرآن)، دار المعرفة، بيروت.

﴿ ك ﴾

- الكاساني، علاء الدين أبو بكر بن مسعود الكاساني، بدائع الصنائع في ترتيب الشرائع، دار الكتب العلمية، بيروت، لبنان.

﴿ م ﴾

- مأمون محمد سلامة، أصول علم الإجرام والعقاب، دار الفكر العربي، القاهرة، بدون سنة النشر.
- مأمون وجيه الرفاعي، فقه العقوبات، جامعة النجاح الوطنية، 2004م.
- الماوردي، أبو الحسن علي بن محمد الماوردي، الحاوي الكبير، تحقيق علي معوض، وعادل عبد الجواد، دار الكتب العلمية، بيروت، لبنان.
- الماوردي، الأحكام السلطانية، ط1، دار التراث العربي، القاهرة، 1407هـ.
- المباركفوري، أبو العلا محمد عبد الرحمن بن عبد الرحيم المباركفوري، تحفة الأحوذي شرح جامع الترمذي، دار الفكر، بيروت، لبنان، 1415هـ.
- محسن بن سليمان خليفة، جرائم الحاسب الآلي وعقوبتها في الفقه والنظام، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، الرياض 1423هـ .
- محمد أبو العلا عقيدة، أصول علم العقاب، مطابع جامعة عين شمس، دار الفكر العربي، 1997م.
- محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي، كتاب الجريمة، دار الفكر العربي، القاهرة، 1998م..
- محمد أبو زهرة، الحاسوب والقانون، مؤسسة الكويت للتقدم العلمي، الكويت، 1995م.
- محمد أحمد المشهداني، الوجيز في شرح التشريع الجنائي الإسلامي، ط1، مؤسسة الوراق للنشر والتوزيع، عمان، 2004م.
- محمد الألفي، جرائم الانترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، 2008م.
- محمد الألفي، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت، المكتب المصري الحديث للنشر، القاهرة، 2005.
- محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004م.

- محمد الباشا، المعجم الكافي، شركة المطبوعات للنشر والتوزيع، 1994م.
- محمد الدغمي، التجسس وأحكامه في الشريعة الإسلامية، دار السلام للطباعة والنشر والتوزيع، القاهرة، 1985م.
- محمد الدغمي، التجسس وأحكامه في الشريعة الإسلامية، دار السلام للطباعة والنشر، القاهرة، 1985م.
- محمد الرصاع، شرح حدود ابن عرفة ، ط1، دار الغرب الإسلامي، بيروت، 1993م.
- محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، 2008م.
- محمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر، عمان، 2004.
- محمد الفتوحي، منتهى الإرادات في جمع المقنع مع التنقيح وزيادات، ط1، مؤسسة الرسالة، بيروت، 1421هـ ـ 2000م.
- محمد المدني بوساق، محاضرات في مبادئ التشريع الإسلامي، معهد الدراسات العليا، أكاديمية نايف العربية للعلوم الأمنية، الرياض.
- محمد المناصير، الإعلانات التجارية مفهومها وأحكامها في الفقه الإسلامي، أطروحة دكتوراه غير منشورة، كلية الدراسات العليا، الجامعة الأردنية، 2007م.
- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004.
- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، درا المطبوعات الجامعية، الإسكندرية 2003م.
- محمد بن أحمد الأزهري، تهذيب اللغة، تحقيق محمد عوض مرعب، دار إحياء التراث العربي، بيروت، ط1، 2001م .
- محمد بن أحمد بن محمد بن رشد (ت 595هـ)، بداية المجتهد ونهاية المقتصد، مكتبة الكليات الأزهرية، مصر، 1386ه1966م.
- محمد بن سعد كاتب الواقدي، الطبقات الكبرى، دار التحرير، القاهرة، 1388 هـ ـ 1968م.
- محمد بن عبد الرحمن السخاوي، الأجوبة المرضية فيما سئل السخاوي عنه من الأحاديث النبوية، تحقيق محمد بن إسحاق محمد إبراهيم، ط1، دار الراية، الرياض، 1418هـ .
- محمد بن عبد الرحمن المغربي، مواهب الجليل شرح مختصر خليل، ط2، دار الفكر، بيروت، 1398هـ.
- محمد بن علي الشوكاني، السيل الجرار المتدفق على حدائق الأزهار، دار ابن كثير، دمشق، بيروت.
- محمد بوساق، اتجاهات السياسة الجنائية المعاصرة ـ دراسة مقارنة ـ، مركز الدراسات والبحوث، الرياض، 2002م.
- محمد بوساق، التعويض عن الضرر في الفقه الإسلامي، دار اشبيليا للنشر، 1419هـ.
- محمد جمال الدين محفوظ، المدخل إلى العقيدة والاستراتيجية العسكرية الإسلامية، الهيئة المصرية العامة للكتاب، 1976م. .

- محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي ، دار الثقافة للطباعة والنشر ،القاهرة 1987 .
- محمد حسين منصور، أحكام البيع التقليدية والإليكترونية والدولية وحماية المستهلك، دار الفكر الجامعي، الاسكندرية، مصر، 2006م.
- محمد حماد مرهج الهيتي، جرائم الحاسوب، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الأولى، دار المنهاج للنشر والتوزيع، عمان، 2006.
- محمد حماد مرهج الهيتي، جرائم الحاسوب، ط1، إدارة المناهج للنشر والتوزيع، عمان، 2006م.
- محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان، الطبعة الأولى، 2007.
- محمد رواس قعله جي، معجم لغة الفقهاء، حامد قنيبي، دار النفائس للطباعة والنشر والتوزيع، بيروت، ط1، 2، 1408هـ ـــ 1988م.
- محمد زكي أبو عامر و فتوح الشاذلي، مبادئ علم الإجرام والعقاب، منشأة المعارف، الإسكندرية، 1985م.
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 2000م.
- محمد سعيد أحمد، أساليب الحماية القانونية، منشأة المعارف، الاسكندرية، 2008.
- محمد سعيد رمضان البوطي، قضايا فقهية معاصرة، مكتبة الفارابي، دمشق، ط1، 1419ه1999م .
- محمد سليم العوا، أصول النظام الجنائي الإسلامي، دار المعارف، القاهرة، 1998م.
- محمد ضياء الدين الريس، الخراج والنظم المالية للدولة الإسلامية، منشورات أسمار، 2005م.
- محمد عبد الله الوريكات، أصول علمي الإجرام والعقاب، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2009م.
- محمد عقلة، نظام الأسرة في الإسلام، مكتبة الرسالة الحديثة، الأردن، عمان، ط.2، 1989م.
- محمد علي الحلبي، شرح قانون العقوبات القسم العام ـــ، دار الثقافة للنشر والتوزيع، عمان 1997م.
- محمد علي العريان، عمليات غسل الأموال وآليات مكافحتها، دار الجامعة الجديدة للنشر، الاسكندرية، 2005.
- محمد عمر الحاجي، غسيل الأموال، دار المكتبي للطباعة والنشر، 2005م.
- محمد فاروق فايد، إنتاج الديدان باستخدام فيجوال بيسك سكريبت Visual Basic Script ، شركة الكتب المصرية للنشر والتوزيع، مصر، 2009م.
- محمد فاروق فايد، تصميم برامج الاختراق والتجسس، شركة الكتب المصرية للنشر والتوزيع، مصر، 2009م.
- محمد فتحي عبد الهادي، المعلومات وتكنولوجيات المعلومات على أعتاب قرن جديد، مكتبة الدار العربية للكتاب، القاهرة، مصر، 2000.
- محمد فتحي عيد، الإنترنت ودوره في انتشار المخدرات، مركز البحوث والدراسات، أكاديمية نايف العربية للعلوم الأمنية، الرياض 2003، ص7.

- محمد قطب، الجرائم المستحدثة وطرق مواجهتها، قراءة في المشهد القانوني والأمني وعلاقته بالشريعة الإسلامية، دار الفجر للنشر والتوزيع، القاهرة،2009م.
- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001.
- محمد محي الدين عوض، السياسة الجنائية، الكتاب الأول، أكاديمية نايف العربية للعلوم الأمنية، 1418هـ.
- محمد محيي الدين عوض، القيم الموجهة للسياسة الجنائية ومشكلاتها المعاصرة، محاضرات بالمعهد العالي للعلوم الأمنية بالمركز العربي للدراسات الأمنية والتدريب، الرياض، 1993م.
- محمد محيي الدين عوض، محاضرات في السياسة الجنائية، دار النهضة العربية، مصر، د.ت.
- محمد مصباح القاضي، التدابير الاحترازية في السياسة الجنائية الوضعية والشرعية، دار النهضة العربية، القاهرة، 1996م.
- محمد مصطفى القللي، المسؤولية الجنائية، مطبعة جامعة فؤاد الأول، القاهرة، 1948م.
- محمد ناصر الدين الألباني، إرواء الغليل في تخريج أحاديث منار السبيل، المكتب الإسلامي، 1458هـ.
- محمد ناصر الدين الألباني، صحيح سن النسائي، ط1، مكتب التربية لدول الخليج، الرياض، 1408هـ ـ 1988م .
- محمد ناصر الدين الألباني، ضعيف الجامع الصغير وزياداته، ط2، المكتب الإسلامي، بيروت، 1408هـ.
- محمد ناصر الدين الألباني، غاية المرام في تخريج أحاديث الحلال والحرام، مكتبة الرشد، بيروت.
- محمد نجيب حسني، الفقه الجنائي الإسلامي، ط1، دار النهضة العربية، القاهرة، 1427هـ.
- محمد نعيم، التشريع الجنائي الإسلامي، مكتبة الخدمات الحديثة، جدة، 1404هـ.
- محمد وهبة الزحيلي، حقوق الإنسان في الإسلام، دار ابن كثير، دمشق، 1997م.
- محمود أحمد طه، شرح قانون العقوبات (القسم الخاص)، ج1، دار النهضة العربية، القاهرة،2001.
- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005م.
- محمود العيني، البناية في شرح الهداية، ط1، دار الفكر للطباعة والنشر، بيروت، 1401هـ ـ 1981م.
- محمود برهان، ظاهرة التشهير بالأشخاص على الانترنت، دار المنارة العربية، حلب، سوريا، 2007م.
- محمود شيت خطاب، الرسول القائد، دار مكتبة الحياة ومكتبة النهضة، ط2، 1960م.
- محمود مصطفى، شرح قانون العقوبات، القسم الخاص، الطبعة الثامنة، دار النهضة العربية، القاهرة، 1984.
- محمود نجيب حسني، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني ، دار النهضة العربية ، بيروت 1969 .
- محمود نجيب حسني، دروس في علم الإجرام والعقاب، دار النهضة العربية، القاهرة، 1988م.

- محمود نجيب حسني، شرح قانون العقوبات اللبناني القسم العام الجزء الأول، منشورات الحلبي الحقوقية، بيروت، 1998م.
- محمود نجيب حسني، شرح قانون العقوبات اللبناني القسم العام، منشورات الحلبي الحقوقية، بيروت، 1998م.
- محمود نجيب حسني، مدخل للفقه الجنائي الإسلامي، دار النهضة العربية، مصر، 2006م.
- محي الدين بن شرف النووي، تهذيب الأسماء واللغات، دار الكتب العلمية، بيروت، لبنان.
- مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية القاهرة، 2000م.
- المراغي؛ أحمد مصطفى: تفسير المراغي، دار الفكر للطباعة، د.م.
- المرداوي، أبو الحسن بن سليمان المرداوي، الإنصاف في معرفة الراجح من الخلاف، تحقيق محمد حسن إسماعيل، دار الكتب العلمية، بيروت.
- المرغياني، علي بن أبي بكر المرغياني، الهداية شرح بداية المبتدي، المكتبة الإسلامية، بيروت، لبنان.
- مسلم، أبو الحسين مسلم بن الحجاج النيسابوري، ت 261هـ، صحيح مسلم، ط2، دار الدعوة، اسطنبول، دار سحنون، تونس، 1413هـ.
- مسلم؛ أبو الحسين بن الحجاج مسلم القشيري النيسابوري: الجامع الصحيح، دار إحياء التراث العربي، بيروت، د.ط. 1954م.
- مصطفى أبو زيد فهمي، النظرية العامة للدولة، منشأة المعارف، الاسكندرية، ط1، 1985م.
- مصطفى الزرقا، المدخل الفقهي العام، دار القلم، دمشق،1998م. .
- ممدوح الشيخ، التجسس التكنولوجي (سرقة الأسرار الاقتصادية والتقنية)، مكتبة بيروت، سلطنة عمان، 2007.
- المنذري؛ أبو محمد عبد العظيم بن عبد القوي: الترغيب والترهيب، ت: إبراهيم شمس الدين، دار الكتب العلمية، بيروت، ط1417هـ.
- منصور بن يونس البهوتي، كشاف القناع عن متن الإقناع، تحقيق هلال مصيلحي، ومصطفى هلال، دار الفكر، بيروت، 1982م.
- منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، 2006م.
- منصور محمد محروس، دليل مواقع الانترنيت، ط2، دار العصر، الرياض، 2000م.
- منير الجنبيهي، وممدوح الجنبيهي، النقود الإلكترونية، دار الفكر الجامعي، الاسكندرية، 2005.
- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي 2004م .
- مهندس انتصار الغريب، أمن الكومبيوتر والقانون، دار الراتب الجامعية، بيروت، لبنان، 1994.
- الموصلي، الاختيار لتعليل المختار، تعليق أبو دقيقة، دار المعرفة، بيروت، لبنان، ط2، 1370هـ ـــ 1951م.

- موفق الدين عبد الله بن أحمد بن قدامة المقدسي، و عبد الرحمن بن محمد بن أحمد ابن قدامة المقدسي، وعلي سليمان المرداوي، المقنع والشرح الكبير ومعهما الإنصاف، تحقيق الدكتور عبد الله بن عبد المحسن التركي، دار هاجر للطباعة والنشر، القاهرة، الطبعة الأولى، 1415هـ.

﴿ ن ﴾

- ناجي معلا، الأصول العلمية للترويج التجاري والإعلان، دار وائل، عمان، 2007م.
- نادر عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، طرابلس، لبنان 2007.
- نادر عبد العزيز شافي، تبييض الأموال، منشورات الحلبل الحقوقية، بيروت 2001م.
- ناصر الدين الألباني، إرواء الغليل، ط1، المكتب الإسلامي 1399هـ ـ 1979م.
- ناصر بن محمد المهيزع، المواد الإباحية والانترنت، مركز أبحاث مكافحة الجريمة، وزارة الداخلية، المملكة السعودية، ب.ت.
- نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، 2005م.
- نبيل عبد المنعم جاد، أسس التحقيق الجنائي لجرائم الحاسب الآلي، مطبعة كلية الشرطة، القاهرة، ب.ت.
- نجيب حسني، علم العقاب، دار النهضة العربية، القاهرة، 1967م، ص 154 .
- نزار فايز أبو علي، فيروسات الكمبيوتر، دار الحنين للنشر، عمان، 1994م.
- النسائي، أبو عبد الرحمن أحمد بن شعيب النسائي، سنن النسائي، دار الدعوة، ودار سحنون، ط2، 1413هـ.
- النسائي؛ أبو عبد الرحمن أحمد بن شعيب: سنن النسائي بشرح السيوطي وحاشية النيسابوري، دار الكتاب العربي، بيروت، لبنان، د.ت.
- نظام المجالي، شرح قانون العقوبات ـ القسم العام ـ، دار الثقافة، عمان، 2005م.
- نظام وآخرون، الفتاوى الهندية في مذهب أبي حنيفة، ط4، دار إحياء التراث، بيروت، 1406هـ ـ 1986م.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008.
- النووي، أبو زكريا محي الدين بن شرف النووي، ت 676هـ، المجموع شرح المهذب، دار الفكر، بيروت.
- النووي، صحيح مسلم بشرح النووي، دار الكتب العلمية، بيروت.
- النووي، روضة الطالبين، تحقيق عادل عبد الجواد وعلي معوض، دار الكتب العلمية، لبنان.
- النووي، المنهاج شرح صحيح مسلم ابن الحجاج، ت: خليل مأمون شيحا، دار المعرفة، بيروت، ط4، 1418هـ ـ 1997م.

﴿ هـ ﴾

- هدى حامد قشقوش، جرائم الحاسب الآلي في القانون المقارن، دار النهضة العربية، مصر، 1992م.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، القاهرة، 1992م.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1993م.
- هلالي عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2007م.

﴿ و ﴾

- الواحدي، أبو الحسن علي بن أحمد، الوجيز في تفسير الكتاب العزيز المعروف بتفسير الواحدي، تحقيق، صفوان عدنان داوودي، ط1، دار القلم، والدار الشامية، بيروت، دمشق، 1415هـ .
- وهبة الزحيلي، أصول الفقه الإسلامي، ط1، دار الفكر، دمشق، سوريا، 1986م.
- وهبة الزحيلي، التفسير المنير في العقيدة والشريعة والمنهج، ط1، دار الفكر، دمشق وبيروت، 1991م.
- وهبة الزحيلي، الفقه الإسلامي وأدلته، ط3، دار الفكر، دمشق، 1409 هـ ـ 1989م .
- وهبة الزحيلي، حكم المصنفات الفنية (برامج الحاسوب)، دار المكتبي للطباعة والنشر، دمشق، سوريا، ط1، 1418هـ.
- وهبة الزحيلي، نظرية الضمان أو أحكام المسئولية المدنية والجنائية في الفقه الإسلامي، دار الفكر، دمشق، 1982م.

﴿ ي ﴾

- ياسر يوسف عبد المعطي، مقدمة في الحاسب الآلي وتطبيقاته، شركة المكتبات الكوينية، الكويت، 1994م.
- يسر أنور علي و آمال عبد الرحيم، أصول علمي الإجرام والعقاب، دار النهضة العربية، القاهرة 1999م.
- يوسف الخياط، لسان العرب المحيط، دار الجيل، بيروت، 1998.
- يوسف أمين شاكر و عمر محمد بن يونس، مكافحة غسل الأموال في التشريع المصري، دار النهضة العربية، القاهرة، 2002.
- يونس محمد عرب، جرائم الكمبيوتر والانترنت، ط1، منشورات اتحاد المصارف العربية، بيروت، 2002م.
- يونس محمد عرب، موسوعة القانون وتقنية المعلومات، ط1، منشورات اتحاد المصارف العربية، بيروت 2002م.

﴿المراجع باللغة الأجنبية﴾

- Jerome Hall (1960) : General Principles of Criminal Law, Second Edition, Indiana polis, Bo bbs Merill.
- Padova (y) : Un aperçue de lutte contre la cyber criminalité en France, R.S.C. 2002.
- Michael Alexender, Computer Crime-Ugly secret for business, Computer World, Vol.Xxiv, N°11, 1990.
- Bart de schutter, La criminalité lieé à l'informatique, R.D.P.C, N°1.
- David Thomson, Current trends in computer control crime, Computer Quarterly, N°1, 1991, p.2
- Nidal el Chaer, La Criminalité informatique devant la justice pénale, Edition Sader 2004, Beyrouth Liban.
- The Internet Strategic Plan: A Step by Step Guide to Connecting your Company, By Martin A. Schulman, John wiley and Sons (1997).
- Parker "Dom B", Fighting computer crime "A new Framework for Protecting information", 1998 .
- Specialize in stealing and selling credit card information from the Internet. Hackers, crackers, phrackers, and more, by Boris Loza, Ph.D., CISSP ,Tego System Inc .
- Use knowledge of the telephone system to make calls at the expense of another person. Hackers, crackers, phrackers, and more, by Boris Loza, Ph.D., CISSP ,Tego System Inc .
- Enjoy breaking into computers and destroying them. Hackers, crackers, phrackers, and more, by Boris Loza, Ph.D., CISSP Tego System Inc.
- Attempt to break codes and foil security systems. Hackers, crackers, phrackers, and more, by Boris Loza, Ph.D., CISSP ,Tego System Inc .
- Novice crackers with limited technical expertise who use simple scripts, programs, and automated tools authored by others to create mischief . Hackers, crackers, phrackers, and more, by Boris Loza, Ph.D., CISSP ,Tego System Inc.
- International Telecommunication Union: measuring the information society, ICT development index, Geneva, 2009.
- Eric Feliol, Philippe Richard, CYBER CRIMINALITE ; Enquete sur les mafias qui envahissent le web, Dunod 2006.
- Benseussan (Alain), « Contribution théorique au Droit de la preuve dans le domaine informatique. Aspects juridiques et solution techniques, expertises ». Paris1990.
- Dr. Brandon S. Centerwall, "Television and violence: the scale of the problem and where to go from here." the Journal of the American Medical Association, June 10 1992.
- Edward Donnerstein, "Pornography and Violence Against Women," Annals of the New York Academy of Science, 1980.
- Dr. William Marshall, "Use of Sexually Explicit Stimuli by Rapists, Child Molesters and Non-Offenders," Journal of Sex Research, 1988.
- Testimony by John B. Rabun, deputy director, National Center for Missing and Exploited Children, before the Subcommittee on Juvenile Justice of the Senate Judiciary Committee, 12 September 1984.

- Victor B. Cline, "Treatment and healing of Pornographic and Sexual Addictions," April 1999.
- Kilpatrick et. Al., "Rape in America: A Report to the Nation," April 23, 1992.
- Lisak, "The Psychological Impact of Sexual Abuse, Content Analysis of Interviews with Male Survivors," Journal of Traumatic Stress, Vol. 7, no. 4: 525-548
- -J.QUIRK et V.TANZI, Il faut intensifier la lutte contre le blanchiment de l'argent, FMI Bulltin, 5 août 1995.
- GAFI-VII, Rapport sur les typologies du blanchiment de l'argent, juin 1996.
- Christopher BLAKESLEY, Les systèmes de justice criminelle face au défie du crime organisé, Rapport général du Colloque préparatoire de l'AIDP sur Les systèmes pénaux à l'épreuve du crime organisé, section II, R.I.D.P. 1998.
- Raymond KENDALL, Interpol et la lutte contre la criminalité organisée transnationale, in ''La criminalité organisée '' sous la direction de Marcel LECLERC, la documentation française (I.H.E.S.I.), 1996.
- Nicolas QUELOZ, Les actions internationales de lutte contre la criminalité organisée, Rev.sc. crim. 1997.
- Sylvie ZEKIC, Approche criminologie du concept de crime organisé, Mémoire D.E.A, Université de Nantes, 1999.
- Raymond GASSIN, Criminologie, Dalloz, 1998.
- Reynald OTTENHOF, Le crime organisé : de la notion criminologique à la notion juridique: in '' Criminalité organisée et ordre dans la société.
- M. Cherif BASSIOUNI & Eduardo VETERE, Organized crime and its transnational manifestations, in M. Cherfi BASSIOUNI, International criminal law, Vol.1, transnational Publishers, 2d ed. New York, 1998.
- Sylvie ZEKIC, Approche criminologique du concept de crime organisé, Mémoire D.E.A, Univ. De Nantes, 1999.
- Jean ZIEGLER, Les seigneurs du crime : Les nouvelles mafia contre la démocratie, Seuil, 1998.
- Ahmed Farouk ZAHER, L e blanchiment de l'argent et la recherche des produits de l'infraction, thèse, Univ. De Nantes, 2001 .
- GAFI, La lutte contre le blanchiment de capitaux, rapport demandé par les chefs d'Etat lors du sommet de l'Arche, Coll. des Rapports officiels, éd. La documentation française, 1990.
- Fabrizio HINNA-DANESI, Mafia – politique – entreprise, P.A., n° 35, mars 1999.
- W. LAGUEUR, Postmodern, Terrorism, Foreign Affairs 1996, Vol.75.
- Phyllis B. Gerstenfeld & Ohters (2002) Hate Online : A Content Analysis of Extremist Internet Sites In Analyses of Social Issues and Public Policy, Vol.3, N°.1, 2003.
- D.E . Denning , " The Future Of Cryptography ", Georgetown University , revised jan 6 , 1996.
- Yasinsac, A., Erbacher, R., Marks, D., Pollit, M., and Sommer, P.(2003). ''Computer Forensics Educatin''. IEEE Security & Privacy, July/Agust 2003.
- Gottschalk L., Liu J., Dathan B. , Fitzgerald S. and Stein M., (2005), ''Computer Forensics programs in higher education : a prelimminary study'', Sig CSE'05.
- Isner J. (2003). ''computer Forensics : An Emerging Practice in the Battle Against Cyber Crime'', SANS Institute, Bethesda, Maryland.

- Peterson G. L., Raines R. A. and Baldwin R. O., (2007). ''Graduate Digital Forensics Education at the Air Force Institute of Technology''. In HICCSS '07: Proceedings of the 40th Annual Hawaii International Conference on system Sciences. IEEE Computer society.
- Vacca, John (2002), Computer Forensics : Computer Crime Scene Investigation, Hingham, Massachusetts : Charles River Media.
- Mandia K. & Prosie C. (2001). Incident Response : Investigation Computer Crime. Berkeley, California : McGraw-Hill.
- Shinder, Derba (2002). Scene of The Cybercrime : Computer Forensics Handbook. Rockland, MA : Syngress Publishing.
- Sammes T. & Jenkinson B. (2002). Forensic Computing : A practitioner's Guide, London : Springer.
- Mandia K. & Prosise C. (2001). Incident Response : Investigating Computer Crime. Berkeley, Clifornia : McGraw-Hill.
- Stephenson Peter (2000). Investigating Computer-Related Crime, Boca Raton Florida : CRC Press.
- Sammes T. & Jenkinson B. (2002). Forensic Computing : A practitioner's Guide, London : Springer.
- Shinder, Derba (2002). Scene of The Cybercrime : Computer Forensics Handbook. Rockland, MA : Syngress Publishing.
- Gibbs (J.) Mazan (K.), Electronic Signatures, Understanding FDA's Electronic Records and Signatures regulation, Medical Devise & Diagnostic Industry Magazine, May 1999.
- Lillian Edwards & Charlotte Waelde, Law and the Intenet, Framework of electronic Commerce, HART publishing Oxford Second Edition, 2000.
- David Johston Sunny Handa,Cyber Law, what you need toknow about doing business on line second edition 2002.
- European Commission: Proposal for European parliament and council directives on the taking up, the pursuit and prudential supervision of the business of electronic money institution. Brussels, 1998, COM(98) .
- Bank for International Settlements (BIS),(1996), Implication for Central Banks of the development of Electronic Money. Basle.

- إبراهيم رافعة الحمداني، أثر استخدام التكنولوجيا المصرفية في ظاهرة غسيل الأموال والجهود الدولية لمكافحتها، ورقة عمل مقدمة للمؤتمر العلمي الرابع "الريادة والإبداع" استراتيجيات الأعمال في مواجهة تحديات العولمة، جامعة فيلادلفيا، عمان الأردن 2005.
- إبراهيم محمد بركات، أهمية الإفصاح عن مخاطر المعاملات المالية المتعلقة بغسل الأموال في البنوك التجارية، دراسة تحليلية في ضوء نظرية المسؤولية الاجتماعية؛ بحث مقدم للمؤتمر العلمي السنوي السابع إدارة المخاطر واقتصاد المعرفة، المحور السابع: إدارة المخاطر والمحاسبة، جامعة الزيتونة الأردنية، عمان الأردن 16 18 نيسان 2007.
- أبو هيبة، نجوى، التوقيع الإلكتروني تعريف ومدى حجيته في الإثبات، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، تنظيم كلية الشريعة والقانون بجامعة الإمارات وغرفة التجارة والصناعة بدبي، للفترة 10 12 ماي 2003.
- أحمد سليمان الزغاليل، الاتجار بالنساء والأطفال، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، 1420هـ.
- الرائد علي حسن عباس، مخاطر استخدام بطاقات الدفع الإلكتروني عبر شبكة الانترنت (المشاكل والحلول)، ورقة عمل مقدمة إلى ندوة "الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني" التي نظمها مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة 14 ديسمبر 1998.
- القاضي وليد عالكوم، التحقيق في جرائم الحاسوب، بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، شرطة دبي، أفريل 2003، المجلد الأول.
- القاضي وليد عالكوم، مفهوم وظاهرة الإجرام المعلوماتي، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنيت، جامعة الإمارات، 2000م.
- محمد عوض، تعريف الإرهاب، بحث مقدم للندوة العلمية الخمسون حول تشريعات مكافحة الإرهاب في الوطن العربي، جامعة نايف العربية للعلوم الأمينة.
- علي الخليل، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة

والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3 ماي 2000م.

- عزيزة الشريف، الظواهر الاقتصادية والسياسية للعولمة (ظاهرة غسل الأموال وأثرها على الاقتصاد الوطني)، مؤتمر التأثيرات القانونية والاقتصادية والسياسية للعولمة على مصر والعالم العربي، كلية الحقوق، جامعة المنصورة، المؤتمر السنوي السادس، القاهرة، 26- 27 مارس 2002م.
- بيان مكة المكرمة الصادر عن المجمع الفقهي لرابطة العالم الإسلامي ، الدورة السادسة عشرة ، مكة المكرمة ، رابطة العالم الإسلامي 1422هـ.
- صلاح زين الدين، دراسة اقتصادية لبعض مشكلات وسائل الدفع الإلكترونية، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة القانون، دبي، 2003.
- عبد الرحمن السند، وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها، بحث مقدم للمؤتمر العالمي عن موقع الإسلام من الإرهاب، جامعة الإمام محمد بن سعود، الرياض، المملكة العربية السعودية، 2004م.
- عبد الله حسين محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات ، بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، شرطة دبي، أفريل 2003، المجلد الأول.
- علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، في جامعة الإمارات العربية المتحدة، عام 2000م.
- علي عبد القادر القهوجي، الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، بحث مقدم لمؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، دبي الإمارات العربية المتحدة، 26-28 ابريل2003، أكاديمية شرطة دبي.
- عماد علي الخليل، التكيف القانون لإساءة استخدام أرقام البطاقات الائتمانية عبر شبكة الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة من 1 3 ماي 2000م، المجلد الثاني.
- غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنيت، كلية الشريعة والقانون، جامعة الإمارات، ماي 2000م.
- غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات، كلية الشريعة والقانون، عام 2000.

- غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنيت، كلية الشريعة والقانون، جامعة الإمارات، سنة 2000م.
- فايز بن عبد الله الشهري، ثقافة التطرف على شبكة الإنترنت الملامح والاتجاهات، الندوة العلمية استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 25 – 27 أكتوبر 2010.
- محمد إبراهيم أبو شادي، الصورة المستحدثة لجرائم بطاقات الدفع الإلكتروني واستراتيجية مواجهتها، ورقة عمل مقدمة إلى ندوة "الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني" التي نظمها مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة في 14 ديسمبر 1998م.
- محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول: الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، الإمارات العربية المتحدة، المجلد الأول، ص 19، أبريل 2003.
- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات العربية، ماي 2000م.
- محمد عبد الرحيم سلطان، جرائم الانترنيت والاحتساب عليها، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنيت، جامعة الإمارات، 2000م.
- محمد عبد العزيز العقيل، التحريض الإلكتروني على الإرهاب، بحث نشر بمناسبة مؤتمر: دور الإعلام العربي في التصدي لظاهرة الإرهاب، الذي نظمته جامعة نايف للعلوم الأمنية بالتعاون مع الأمانة العامة لمجلس وزراء الإعلام العرب.
- مصطفى محمد موسى، التنظيمات الإرهابية وشبكة الإنترنت، الندوة العلمية استشراف التهديدات الإرهابية، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 20 22 أوت 2007.
- ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلوماتية العالمية الجريمة عبر الانترنيت منظور أمني ـــ، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنيت، جامعة الإمارات، 2000م.
- موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، 2009م.

- نائل عبد الرحمن صالح: واقع جرائم الحاسوب في التشريع الأردني، بحث مطبوع قدم إلى مؤتمر القانون والكومبيوتر والانترنيت، كلية الشريعة والقانون، جامعة الإمارات، ماي 2000م.
- هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد بالقاهرة من 25 28 أكتوبر 1993م.
- هشام فريد رستم، الجرائم المعلوماتية: أصول التحقيق الجنائي الفني واقتراح بانشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنيت، جامعة الإمارات، 2000م.
- هلالي عبد الله أحمد، حجية المخرجات الكومبيوترية في المواد الجنائية، دراسة مقارنة، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنيت. كلية الشريعة والقانون، جامعة الإمارات، ماي 2000م.
- وليد عاكوم، "مفهوم وظاهرة الإجرام المعلوماتي" ، مؤتمر القانون والكومبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية الممتحنة، المنعقد في 1 3 ماي 2000، المجلد الأول، الطبعة الثالثة، 2004.
- يونس عرب، الاتجاهات التشريعية للجرائم الإلكترونية، ورقة عمل مقدمة لورشة " تطوير التشريعات في مجال مكافحة الجرائم الالكترونية " المنظمة من طرف هيئة تنظيم الاتصالات، مسقط سلطنة عمان 2ـــ4 أفريل 2006.

﴿المجلات والدوريات﴾

- إبراهيم بعزيز، الدول العربية ومجتمع المعلومات، التحديات والفرص المتاحة، المجلة العربية للاتصال والتنمية، ع1، تشرين الأول 2010م.
- أحمد السمدان، مجلة الحقوق، مجلة فصلية محكمة تعني بالدراسات القانونية والشرعية، النظام القانوني لحماية برامج الكمبيوتر، الكويت، العدد الرابع، السنة الحادية عشر، 1408هـــ.
- أسامة بن غانم العبيدي، جرائم الحاسب الآلي والانترنت: الصعوبات التي تعترض المكافحة، دورية الإدارة العامة، معهد الإدارة العامة، المجلد الثامن والأربعون، العدد الأول، يناير 2008م.
- رياض منصور الخليفي، القاعدة الفقهية حجيتها وضوابط الاستدلال بها، مجلة الشريعة والدراسات الإسلامية الكويتية، العدد55، شوال 1424هـــ.
- مجلة البحوث الإسلامية، الرئاسة العامة للبحوث الإسلامية والإفتاء، المملكة العربية السعودية، من ربيع الأول إلى جمادى الثانية 1423هـــ، رقم 66.

- عبد العزيز أحمد بن حسين، المخدرات وظاهرة غسل الأموال، مجلة الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، العدد 2004، السنة الثانية عشرة، 1999م. .
- جرائم الحاسب، مقال منشور في مجلة عربيوتر (مجلة شهرية تعني بعلوم الحاسوب)، الرياض، العدد 40، أوت 1993م.
- حسن بن أحمد الشهري، الأنظمة الإلكترونية الرقمية المطورة لحفظ وسرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56، الرياض، 2012م.
- حميد الجميلي، عمليات غسيل الأموال القذرة تجتاح الاقتصاد العالمي، مجلة الحكمة، العدد 19، السنة الرابعة، بيت الحكمة، 2001م.
- صبحي الأعشى، المجلة العسكرية الأردنية، عدد 43، أوت 1965.
- عبد المجيد الصلاحين، الإعلانات التجارية أحكامها وضوابطها في الفقه الإسلامي، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد 21، السنة الثالثة عشر، 1425 هـ ـ 2004م.
- عبد المجيد الصلاحين، الإعلانات التجارية أحكامها وضوابطها في الفقه الإسلامي، مجلة الشريعة والقانون، العدد 21، السنة الثالثة عشر، ص 37، وعبد الرحمن بن حسن النفيسة، الإعلان التجاري وبعض ما يترتب عليه من أحكام، مجلة البحوث الفقهية المعاصرة، العدد14.
- عصام أحمد فريحات، إعداد القوى العاملة لمجتمع المعلومات، مجلة المعلوماتية، تصدر دوريا عن الجمعية العلمية السورية للمعلوماتية، عدد 09،(2005م، 1426 هـ).
- علي أحمد، غسيل الأموال، مجلة الدراسات الإسلامية والعربية، العدد 25، 1424هـ ـ 2003م. .
- علي أحمد، غسيل الأموال، مجلة كلية الدراسات الإسلامية والعربية، العدد 25، 1424هـ ـ 2003م.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية التي تصدرها كلية الحقوق بجامعة الإسكندرية، الإسكندرية، 1992م.
- محمد البشرى، التحقيق في جرائم الحاسب والانترنت، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 30، الرياض، نوفمبر 2000م.
- فاضل داود علي، أسباب الجريمة، مجلة المنهل الشهرية للآداب والعلوم الثقافية، جدة، العدد 346، 1985م.
- فلاح حسن ثوبني، باسم عبد الهادي، ظاهرة غسيل الأموال وأثارها على الصعيد الدولي، مجلة كلية الإدارة والاقتصاد، الجامعة المستنصرية، بغداد، العراق، العدد 40، 2002. .
- مجلة الجيش اللبنانية، العدد 308، فيفري 2001، مقال إخباري بعنوان: إمبراطورية الانترنت وفرسان القرصنة.

- مجلة إنترنت العالم العربي، العدد الثامن، جوان 2000م، تصدر من إمارة دبي.
- مجلة إنترنت العالم العربي، العدد الثامن، جوان 2000م، تصدر من إمارة دبي.
- مجلة زهرة الخليج، العدد 1028، الصادرة بتاريخ 1998/12/5.
- مجلة مجمع الفقه الإسلامي ، العدد الخامس ، المجلد الثالث.
- مجلة مجمع الفقه الإسلامي، العدد الخامس، الجزء 3، 1409 هـ.
- محمد السنباطي، موقف الشريعة الإسلامية من جرائم الحاسب الآلي والانترنت، بحث منشور في مجلة الشريعة والقانون، ع24، كلية الشريعة والقانون.
- محمد قطب، جرائم الأخلاق والآداب عبر الشبكة الدولية للمعلومات الانترنت ودور التدريب في مواجهتها، مجلة الأمن العام، العدد 199، السنة 49، 1428هـ أكتوبر 2007م، البحرين.
- موزة المزروعي، الاختراقات الإلكترونية خطر كيف نواجهه، مجلة آفاق اقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر 2000م.
- أحمد عباس الوزان، مستجدات ظاهرة غسيل الأموال قنوات الغسيل سبل المعالجة، مجلة كلية الإدارة والاقتصاد، الجامعة المستنصرية، 2004، بغداد.
- صلاح الدين عبد الحميد عبد المطلب، كيفية الاستفادة من المحاكاة الحاسوبية في أعمال البحث والتحقيق الجنائي، مجلة البحوث الأمنية، م 16، ع38، مركز البحوث والدراسات بكلية الملك فهد الأمنية، الرياض، 2008م.

﴿الرسائل الجامعية﴾

- أحمد بن عبد الله الرشودي، حجية الوسائل الإلكترونية في الإثبات الجنائي، دراسة تأصيلية مقارنة تطبيقية، أطروحة دكتوراه غير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2008م.
- أحمد أمداح، التجارة الإلكترونية من منظور الفقه الإسلامي، رسالة ماجستير في الفقه وأصوله، غير منشورة، جامعة باتنة، الجزائر، 2006م.
- أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي، أطروحة دكتوراه، أكاديمية الشرطة كلية الدراسات العليا، دبي، 2004.
- بيان محمد جميل طحان، دراسة اقتصادية للإعلان في الاقتصاد الإسلامي، رسالة ماجستير غير منشورة، جامعة أم القرى، مكة المكرمة، المملكة العربية السعودية، 1410ه1995م.

- حيان مصباح عيسى، جرائم الحاسب الآلي، بحث علمي قانوني لنيل درجة الدبلوم في القانون الجزائي، جامعة دمشق، كلية الحقوق، 1420هـ.
- رشدي محمد علي، الحماية الجنائية للمعلومات على شبكات الانترنيت، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 2010م.
- عبد الله بن محمد الشهري، المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي، دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض.
- عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت (أطروحة دكتوراه كلية الحقوق ت جامعة عين شمس 2004م) .
- غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية الحاسب والإنترنت أطروحة دكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.
- محمد بن عبد الله بن علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003.
- المري عايض راشد، مدى حجية الوسائل التكنولوجية في إثبات العقود التجارية، القاهرة، جامعة القاهرة، أطروحة دكتوراه غير منشورة، 1988.

﴿الجرائد والصحف﴾

- جريدة الأهرام المصرية العدد 420069 الصادر في 1 فيفري 2002م.
- جريدة الأهرام المصرية، 1999/3/2م، مقال بعنوان: النصب عن طريق الانترنت.
- جريدة الرياض ، العدد 12051 ، يوم الجمعة 1 / ربيع أول / 1420هـ.
- جريدة الرياض السعودية، الصادرة في 30 جانفي 2005م، العدد رقم: 13369 .
- جريدة الرياض السعودية، الملحق الاقتصادي، 2 أوت 2008م، العدد 14649، السنة الخامسة والأربعون.
- جريدة الرياض، العدد 12328 ، الثلاثاء 12 محرم 1423هـ.
- جريدة الرياض، العدد 12624، الخميس 13 ذو القعدة 1423هـ، صفحة انترنت واتصالات، السعودية.

﴿مواقع الانترنت﴾

- http//almoslim.net/node/82023
- http://adala.justice.gov.ma/production/Conventions/ar/Conv_Arabe/CA_Lutte_contre_terrorisme.htm
- http://aitnews.com/2013/07/23
- http://alaanmasr.com/news/6431 .
- http://arareaders.com
- http://computer.atlas4e.com/Project_E1/Project/chapter01/chapter1.htm#1-1
- http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
- http://dictionnaire.phpmyvisites.net
- http://droitpp.blogspot.com/2012/10/blog-post_8.html
- http://eastlaws.com/2010/03/23-11-2001.html
- http://en.wikipedia.org/wiki/File:Internet_users_per_100_inhabitants_ITU.svg
- http://forums.naseej.com/showthread.php?t=88363
- http://globalstudy.bsa.org/2008/studies/globalpiracy2008.pdf&s
- http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html (2013)
- http://islamtoday.net/nawafeth/mobile/zview-58-9622.htm
- http://lifehacker.com/5192415/protect-your-windows-pc-from-the-conficker-worm
- http://news.masrawy.com/masrawynews/
- http://norton.com/cybercrimereport for more information and detailed methodology
- http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/
- http://server7.alriyadh.com.sa/22-05-2000/page20html .
- Http://spyware-review.com/internet-pornograpgy-statistics.html
- Http://spyware-review.com/internet-pornograpgy-statistics.html
- http://tasmem2010.grafbb.com/t17-topic
- http://us.mcafee.com/virusInfo/default.qsp?=calendar.
- http://usinfo.state.gov/journals/itgic/0306/ijga/larkin.htm
- http://whatis.techtarget.com/
- http://writers .alriyadh.com.sa/kpage.asp
- http://www.aawsat.com/details.asp?section=4&issue=9231&article=221762
- http://www.abanet.org/crimjust/fedreport.html.
- http://www.alarabiya.net/ar/north-africa/tunisia/2013/09/21.
- http://www.alarabiya.net/Articles/2006/08/29/27004.htm
- http://www.alarabiya.net/articles/2010/09/26/120392.html
- http://www.aljoumhouria.com
- http://www.almaany.com/ar/dict/ar-ar/
- http://www.almaany.com/ar/dict/ar-ar/
- http://www.alriyadh.com/389426
- http://www.alriyadh.com/389426،

- http://www.alyaseer.net/vb/showthread.php ?t=4882
- http://www.amnesty.org/ar/library/asset/ACT30/005/2010/ar/1747d2e3-89d9-4e59-aa81-f58eb132f1a2/act300052010ara.html
- http://www.commentcamarche.net/contents/1234-chevaux-de-troie-informatique
- http://www.defenselink.mil/nii/org/sio/iptreport4_26dbl.doc
- http://www.echoroukonline.com/ara/articles/161698.html
- http://www.elaph.com/ElaphWeb/InternetNews/2007/1/201575.htm
- http://www.hazemsakeek.com/Scientifc_Asay/internet/security.htm
- http://www.histoire-cigref.org/blog/histoire-des-virus-cauchemars-de-l-informatique /
- http://www.hrw.org/adrocacy/internet/mena/
- http://www.huffingtonpost.co.uk/2013/09/22/pornography-addiction_n_3971551.html
- http://www.ibtimes.co.uk/silk-road-2-0-fbi-shuts-down-illegal-drugs-guns-website-arrests-blake-benthall-1473547
- http://www.ic3.gov
- *http://www.independent.co.uk/life-style/health-and-families/health-news/pornography-addiction-leads-to-same-brain-activity-as-alcoholism-or-drug-abuse-study-shows-8832708.html*
- http://www.internetsociety.org/ar/brief-history-internet
- http://www.internetsociety.org/ar/brief-history-internet
- http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Transition
- http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2htm
- http://www.itp.net/arabic/586177
- http://www.JAAScois.com
- http://www.journal.cybrarians.org/index.php
- http://www.kacst.edu.sa/ar/depts/isu/Pages/about_internet.aspx.
- http://www.Low.Uk.comp
- http://www.mcit.gov.sa/home.asp?1=AR&p=15&r=154
- http://www.minshawi.com/old/internet crim-in%20the%20law.htm
- *http://www.normandoidge.com/normandoidge.com/MAIN.html*
- http://www.odccp.org/palermo/convmain/html
- http://www.richmond.edu/jolt/v7i3/article2.html.
- http://www.saleemnet.com/news/index.php?option=com_content&view=article&id=170:2009-09-01-06-06-24&catid=44:cyber-threats&Itemid=113
- http://www.salvomag.com/new/articles/salvo13/13hilton.php
- http://www.sans.org/infosecFAQ/social/social.htm.
- http://www.sans.org/infosecFAQ/social/social.htm.
- http://www.securityfocus.com/infocus/1527
- http://www.skynewsarabia.com/web/article/367051
- http://www.skynewsarabia.com/web/article/584373
- http://www.tech-wd.com/wd/2013/08/14/spam-report
- http://www.tech-wd.com/wd/2014/01/14
- http://www.un.org/ar

- http://www.unhcr.org/4a2d199b2.html
- http://www.vetogate.com/1324267
- http://www.visionael.com/products/secruity_audit/FBI_CSI_2003.PDF
- http://www.wdl.org/ar/item/11579
- http://zeth.kodslav.org/security/dokumentation/dokumentation/soceng/socialeng.html
  http://www.alyaseer.net/vb/showthread.php ?
- http;//www.Usdoj gov/criminal/fraud/text/internet.html
- https://instec.wordpress.com/2008/06/19/videosub
- mubasher.aljazeera.net/news/2012/06/20126102016225351l8.htm
- Study by Ynkelovich Partners Inc., Sep.1999, Qtd. By Proven Men Ministries, LTD. (www.ProvenMen.org). Web.4dec.2009. (http//www.provenmen.org/framework/index.php?paeg=need)
- www.akhbarelyoum.dz
- www.alriyadh.com/2013/11/07/article881895.html
- www.arablaw.net
- www.childsoldiersglobalreport.org/content/facts-and-figures-child-soldiers،
- www.drak-secrts.com
- www.dw.de
- www.elmustakbal.com/News/17494
- www.et.gov.ae/ar/eservices/pages/auctioncard.aspx
- www.hackers.secrts/credit/credit3txt .
- www.himag.com/articles/art4.cfm?topicid=4&id=938
- www.internetworldstats.com/stats19.htm.
- www.internetworldstats.com/stats7.htm .
- www.pingdom.com .
- www.socialbakers.com/facebook-statistics .
- www.uncjin.org
- www.unictgral.org.
- www.usdoij.gov/criminal/cybercrime/reporting.htm
- www.usinfo.state.gov
- www.witsa.orgAlliance

فهرس الموضوعات

الموضوع	الصفحة
مقدمة.	أ
الباب الأول: مفاهيم الدراسة	
الفصل الأول: مفهوم الجريمة الإلكترونية والفقه الجنائي الإسلامي	3
المبحث الأول: مفهوم الجريمة في اللغة والاصطلاح	4
المطلب الأول: التعريف اللغوي للجريمة	4
المطلب الثاني: مفهوم الجريمة في الفقه الجنائي الإسلامي	5
المطلب الثالث: أركان الجريمة في الفقه الجنائي الإسلامي	8
المطلب الرابع: المفهوم الوضعي للجريمة	13
المبحث الثاني: مفهوم الجريمة الالكترونية، خصائصها وأركانها.	17
المطلب الأول: مفهوم الجريمة الإلكترونية في اللوائح والقوانين الوضعية	17
المطلب الثاني: خصائص الجريمة الإلكترونية	23
المطلب الثالث: أركان الجريمة الإلكترونية	25
المبحث الثالث: مفهوم الفقه الجنائي الإسلامي	28
المطلب الأول: مفهوم الفقه الإسلامي	28
المطلب الثاني: مفهوم الفقه الجنائي الإسلامي ومدلولاته	33
المطلب الثالث: مفهوم العقوبة ومقاصدها في الفقه الجنائي الإسلامي	34
الفصل الثاني: أدوات الجريمة الالكترونية	37
المبحث الأول: الحاسوب، تعريفه، نشأته وأهميته	38
المطلب الأول: مفهوم الحاسوب ونشأته	38
المطلب الثاني: دور الحاسوب في الجريمة الإلكترونية	44
المطلب الثالث: برامج الحاسوب	46
المبحث الثاني: شبكة المعلومات العالمية	50
المطلب الأول: مفهوم شبكة الانترنت لغة واصطلاحا	50
المطلب الثاني: تاريخ نشأة الانترنت وخصائصها	52
الفصل الثالث: المجرم المعلوماتي وعلاقته بالجريمة الإلكترونية	60
المبحث الأول: المفهوم العام للمجرم وسيكولوجيته	61
المطلب الأول: تعريف المجرم في اللغة والاصطلاح	61

الموضوع	الصفحة
المطلب الثاني: مفهوم المجرم في علم الإجرام	63
المبحث الثاني: سمات المجرم المعلوماتي وتصنيفاته	65
المطلب الأول: سمات المجرم المعلوماتي	66
المطلب الثاني: دوافع الجرائم الإلكترونية	67
المطلب الثالث: تصنيفات المجرم المعلوماتي	70
المبحث الثالث: المجرم المعلوماتي والهندسة الاجتماعية	76
المطلب الأول: طرق الهندسة الاجتماعية	76
الفصل الرابع: المجتمع المعلوماتي ومؤشراته	81
المبحث الأول: مفهوم المجتمع المعلوماتي	83
المطلب الأول: التعريف الاصطلاحي للمجتمع المعلوماتي	83
المطلب الثاني: أسباب نشوء مجتمع المعلومات	84
المطلب الثالث: خصائص مجتمع المعلومات	86
المبحث الثاني: المؤشرات الإحصائية للمجتمع المعلوماتي	87
المطلب الأول: تعداد مستخدمي الانترنت ونطاقاتها	87
المطلب الثاني: تعداد مستعملي تطبيقات الشبكات	89
المطلب الثالث:مؤشرات المجتمع المعلوماتي في العالم العربي	93
الباب الثاني : أنواع الجرائم الالكترونية وآثارها	
الفصل الأول: الجرائم الإلكترونية المتعلقة بأمن المعلومات	101
المبحث الأول: الجرائم المستهدفة للحواسيب	102
المطلب الأول: جريمة الدخول غير المصرح به إلى الحاسوب	102
المطلب الثاني: أركان جريمة الدخول غير المشروع للحواسيب	103
المطلب الثالث: صور الدخول غير المشروع للحاسوب وآثارها	104
المبحث الثاني: جرائم تطوير الفيروسات ونشرها	108
المطلب الأول: مفهوم الفيروس في المجال المعلوماتي	108
المطلب الثاني: أنواع فيروسات الحواسيب	111
المبحث الثالث: جرائم تدمير المواقع الإلكترونية	116
المطلب الأول: أشكال تدمير المواقع الإلكترونية	116
المطلب الثاني: أهداف تدمير المواقع الإلكترونية	117

الموضوع	الصفحة
المبحث الرابع: جرائم اختراق البريد الإلكتروني وقرصنة البرامج	119
المطلب الأول: صور اختراق البريد الإلكتروني	119
المطلب الثاني: أهداف اختراق البريد الإلكتروني	120
المطلب الثالث: جريمة قرصنة البرامج وصورها	121
المبحث الخامس: جريمة التزوير الإلكتروني	123
المطلب الأول: مفهوم التزوير الإلكتروني	123
المطلب الثاني: أساليب وصور جريمة التزوير الإلكتروني	125
الفصل الثاني: الجرائم الإلكترونية المتعلقة بالأموال والأشخاص	127
المبحث الأول: الجرائم الإلكترونية المتعلقة بالأموال	128
المطلب الأول: مفهوم جريمة الاختلاس الالكتروني للأموال	128
المطلب الثاني: صور جرائم الاختلاس الإلكتروني للأموال	130
المطلب الثالث: جريمة غسيل الأموال الإلكترونية	140
المبحث الثاني: الجرائم الإلكترونية المتعلقة بالأشخاص والآداب العامة	147
المطلب الأول: صور الجرائم الإلكترونية المتعلقة بالأشخاص	147
المطلب الثاني: صور الجرائم الإلكترونية المتعلقة بالآداب العامة	151
الفصل الثالث: الجرائم الإلكترونية المتعلقة بأمن الدول والمجتمعات	159
المبحث الأول: جرائم التجسس الإلكتروني	160
المطلب الأول: مفهوم التجسس وأنواعه	160
المطلب الثاني: صور التجسس الإلكتروني وآثاره	166
المبحث الثاني: الجريمة المنظمة عبر الانترنت.	169
المطلب الأول: مفهوم الجريمة المنظمة	169
المطلب الثاني: خصائص الجريمة المنظمة	172
المطلب الثالث: أبعاد الجريمة المنظمة في الفضاء الإلكتروني	174
المبحث الثالث:الإرهـــــاب الإلكتـــروني	178
المطلب الأول: مفهوم الإرهاب الإلكتروني	178
المطلب الثاني: خصائص الإرهاب الإلكتروني وأهدافه	181
المطلب الثالث: صور الإرهاب الإلكتروني	182

الموضوع	الصفحة

الباب الثالث: الآليات الفنية والتشريعات القانونية لمكافحة الجريمة الإلكترونية

الفصل الأول: الإجراءات الفنية لمكافحة الجريمة الإلكترونية 191

المبحث الأول: مفهوم أمن المعلومات 192

المطلب الأول: مفهوم أمن المعلومات 192

المطلب الثاني: المهام الرئيسية لأمن المعلومات 193

المبحث الثاني: الوسائل التقنية لأمن المعلومات 195

المطلب الأول: البرامج المضادة للفيروسات 195

المطلب الثاني: الجدران النارية 197

المطلب الثالث: تشفير البيانات 201

المطلب الرابع: التوقيع الإلكتروني 204

المبحث الثالث:الحاسوب الجنائي ودوره في أمن المعلومات 213

المطلب الأول: مفهوم الحاسوب الجنائي ومنهجيته 213

المطلب الثاني: برامج الحاسوب الجنائي التطبيقية 216

الفصل الثاني: التدابير والتشريعات القانونية لمكافحة الجريمة الإلكترونية 222

المبحث الأول: مفهوم القانون الجنائي وصوره الجزائية 223

المطلب الأول: مفهوم القانون الجنائي 223

المطلب الثاني: الجزاء الجنائي وصوره 224

المطلب الثالث: العلاقة بين العقوبة والتدابير الاحترازية 234

المبحث الثاني: التشريعات القانونية الإقليمية تجاه الجرائم الإلكترونية 235

المطلب الأول: نماذج من الدول الأجنبية 236

المطلب الثاني: نماذج من الأطر القانونية لمكافحة الجرائم الإلكترونية في الدول العربية 247

المبحث الثالث: التدابير والمعاهدات الدولية لمكافحة الجرائم الإلكترونية 266

المطلب الأول: القرارات والإجراءات الدولية لمكافحة الجرائم الإلكترونية 266

المطلب الثاني: اتفاقية بودابست لمكافحة الجرائم الإلكترونية 270

المطلب الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 276

الباب الرابع: المسؤولية الجنائية عن الجرائم الإلكترونية في التشريع الجنائي الإسلامي

الفصل الأول: جرائم الاعتداء على المال وحكمها في الفقه الجنائي الإسلامي 286

المبحث الأول: جرائم التعدي على الحاسوب والبرامج 287

المطلب الأول: جريمة التعدي على معلومات الحاسوب 287

الموضوع	الصفحة
المطلب الثاني: جريمة التعدي على برامج الحاسوب	294
المطلب الثالث: جريمة إنشاء ونشر الفيروسات الإلكترونية	305
المبحث الثاني: جرائم التعدي على المواقع الإلكترونية	308
المطلب الأول: مفهوم المواقع الإلكترونية	308
المطلب الثاني: حكم التعدي على المواقع الإلكترونية	310
المبحث الثالث: جرائم التزوير الإلكتروني	316
المطلب الأول: مفهوم التزوير الإلكتروني	316
المطلب الثاني: طبيعة المحررات الإلكترونية	318
المطلب الثالث: حكم التزوير وأدلته	323
المطلب الرابع: عقوبة التزوير في الفقه الإسلامي	325
المطلب الخامس: حكم التزوير الإلكتروني	327
المبحث الرابع: جرائم التعدي على النقود الإلكترونية	329
المطلب الأول: مفهوم النقود الإلكترونية	329
المطلب الثاني: مدى مشروعية النقود الإلكترونية وحكم التعدي عليها	334
المبحث الخامس: جرائم التعدي على التجارة الإلكترونية	339
المطلب الأول: مفهوم التجارة الإلكترونية وفوائدها	339
المطلب الثاني: الإعلانات التجارية الكاذبة	342
الفصل الثاني: جرائم الاعتداء على النفس والعرض وحكمها في الفقه الجنائي الإسلامي	351
المبحث الأول: القذف والتشهير الإلكتروني	352
المطلب الأول: مفهوم القذف الإلكتروني وحكمه	353
المطلب الثاني: مفهوم التشهير الإلكتروني وحكمه	356
المبحث الثاني: جرائم التعدي على البريد الإلكتروني	360
المطلب الأول: مفهوم البريد الإلكتروني لغة واصطلاحا	360
المطلب الثاني: صور التعدي على البريد الإلكتروني	362
المطلب الثالث: أهداف التعدي على البريد الإلكتروني	364
المطلب الرابع: حكم التعدي على البريد الإلكتروني	365
المبحث الثالث: جريمة صناعة المواقع الإباحية وترويجها عبر الانترنت	368
المطلب الأول: مفهوم الإباحية وأثرها على الفرد والمجتمع	369

الموضوع	الصفحة
الفصل الثالث: جرائم التعدي على أمن الدولة والمجتمع وحكمها في الفقه الجنائي الإسلامي	377
المبحث الأول: جرائـــم التجسس الإلكتروني	378
المطلب الأول: مفهوم التجسس الإلكتروني	378
المطلب الثاني: أنواع التجسس وأحكامه	380
المطلب الثالث: حكم التجسس الإلكتروني في الفقه الجنائي الإسلامي	386
المبحث الثاني: جريمة غسيل الأموال عن طريق الانترنت	390
المطلب الأول: مفهوم غسيل الأموال	391
المطلب الثاني: الآثار المترتبة على جريمة غسيل الأموال	395
المطلب الثالث: حكم جريمة غسيل الأموال عبر الانترنت	399
المبحث الثالث: جرائم الإرهاب الإلكتروني	403
المطلب الأول: مدلول الإرهاب في اللغة والاصطلاح	403
المطلب الثاني: حكم الإرهاب باعتبار علاقته بالحرابة	411
المطلب الثالث: حكم الإرهاب باعتبار علاقته بالبغي	414
المطلب الرابع: حكم الإرهاب الإلكتروني	418
خاتمة.	421
التوصيات.	423
الفهارس العامة:	
فهرس الآيات القرآنية الكريمة	426
فهرس الأحاديث النبوية الشريفة	434
فهرس الجداول	438
فهرس الأشكال والبيانات	439
فهرس المصادر والمراجع	441
فهرس الموضوعات	479
الملاحق	485
الملخص	

الملاحق

ملحق خاص بنظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية

بسم الله الرحمن الرحيم

المملكة العربية السعودية
هيئة الخبراء بمجلس الوزراء

الرقم : _____
التاريخ : / / ١٤هـ
المرفقات : _____

نظام مكافحة جرائم المعلوماتية

المادة الأولى :

يقصد بالألفاظ والعبارات الآتية - أينما وردت في هذا النظام - المعاني المبينة أمامها ما لم يقتض السياق خلاف ذلك:

١- الشخص: أي شخص ذي صفة طبيعية أو اعتبارية ، عامة أو خاصة .

٢- النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

٣- الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت).

٤- البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

٥- برامج الحاسب الآلي: مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.

٦- الحاسب الآلي: أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات ، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها ، يؤدي وظائف محددة بحسب البرامج ، والأوامر المعطاة له.

٧- الدخول غير المشروع: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

٨- الجريمة المعلوماتية: أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

٩- الموقع الإلكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

١٠- الالتقاط: مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح .

المادة الثانية :

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبما يؤدي إلى ما يأتي :

١ - المساعدة على تحقيق الأمن المعلوماتي.

٢ - حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية .

٣ - حماية المصلحة العامة، والأخلاق، والآداب العامة.

٤ - حماية الاقتصاد الوطني.

المادة الثالثة :

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.

٢- الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً .

٣- الدخول غير المشروع إلى موقع الكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه .

٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا ،أو ما في حكمها .

٥- التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة .

المادة الرابعة :

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .

٢- الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

المادة الخامسة :

يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها .

٢- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أوحذفها، أو تسريبها، أو إتلافها، أو تعديلها.

٣- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت .

المادة السادسة :

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١- إنتاج ما من شأنه المساس بالنظام العام ، او القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده ، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي .

٢ - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار في الجنس البشري، أو تسهيل التعامل به.

٣- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها .

٤- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها .

المادة السابعة :

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

١- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية .

٢- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني .

المادة الثامنة :

لاتقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:

١- ارتكاب الجاني الجريمة من خلال عصابة منظمة .

٢- شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.

٣- التغرير بالقصر ومن في حكمهم، واستغلالهم .

٤- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المادة التاسعة :

يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية .

المادة العاشرة :

يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة .

المادة الحادية عشرة :

للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

المادة الثانية عشرة :

لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفاً فيها.

المادة الثالثة عشرة :

مع عدم الإخلال بحقوق حسني النية ، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها . كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمه إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه.

المادة الرابعة عشرة:

تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة .

المادة الخامسة عشرة :

تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام.

المادة السادسة عشرة :

ينشر هذا النظام في الجريدة الرسمية ويعمل به بعد (مائة وعشرين) يوماً من تاريخ نشره .

ملحق خاص بالقانون الاتحادي رقم 2 لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات الإماراتي

قانون اتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات الاماراتي

http://theuaelaw.com/vb/showthread.php?t=1022

"منشور في العدد رقم (442) من الجريدة الرسمية"

نحن خليفة بن زايد آل نهيان، رئيس دولة الإمارات العربية المتحدة،
بعد الإطلاع على الدستور،
وعلى القانون الاتحادي رقم (1) لسنة 1972 بشأن اختصاصات الوزارات وصلاحيات الوزراء والقوانين المعدلة له،
وعلى القانون الاتحادي رقم (9) لسنة 1976 في شأن الأحداث الجانحين والمشردين،
وعلى القانون الاتحادي رقم (10) لسنة 1980 في شأن المصرف المركزي والنظام النقدي وتنظيم المهنة المصرفية والقوانين المعدلة له،
وعلى القانون الاتحادي رقم (15) لسنة 1980 في شأن المطبوعات والنشر،
وعلى القانون الاتحادي رقم (3) لسنة 1982 بإنشاء المركز الوطني للحاسب الآلي والقوانين المعدلة له،
وعلى قانون العقوبات الصادر بالقانون الاتحادي رقم (3) لسنة 1987 والقوانين المعدلة له،
وعلى قانون الإجراءات الجزائية الصادر بالقانون الاتحادي رقم (35) لسنة1992،
وعلى القانون الاتحادي رقم (37) لسنة 1992 في شأن العلامات التجارية والقوانين المعدلة له،
وعلى القانون الاتحادي رقم (44) لسنة 1992 في شأن تنظيم وحماية الملكية الصناعية لبراءات الاختراع والرسوم والنماذج الصناعية،
وعلى القانون الاتحادي رقم (4) لسنة 2002 في شأن تجريم غسل الأموال،
وعلى القانون الاتحادي رقم (7) لسنة 2002 في شأن حقوق المؤلف والحقوق المجاورة،
وعلى المرسوم بقانون اتحادي رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات،

وبناء على ما عرضه وزير العدل والشؤون الإسلامية والأوقاف، وموافقة مجلس الوزراء، وتصديق المجلس الأعلى للاتحاد،

أصدرنا القانون الآتي:

المادة (1):

تعريفات:

في تطبيق أحكام هذا القانون يقصد بالكلمات والعبارات التالية، المعاني الموضحة قرين كل منها ما لم يقض سياق النص بغير ذلك:

الدولة: دولة الإمارات العربية المتحدة.
المعلومات الالكترونية: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.

البرنامج المعلوماتي: مجموعة من البيانات والتعليمات والأوامر، قابلة للتنفيذ بوسائل تقنية المعلومات ومعدة لإنجاز مهمة ما.

نظام المعلومات الإلكتروني: مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الالكترونية أو غير ذلك.

الشبكة المعلوماتية: ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها.

المستند الإلكتروني : سجل أو مستند يتم انشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة الكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه.

الموقع: مكان إتاحة المعلومات على الشبكة المعلوماتية.

وسيلة تقنية المعلومات: أية أداة الكترونية مغناطيسية، بصرية، كهروكيميائية أو أية أداة أخرى تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، ويشمل أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة.

البيانات الحكومية: ويشمل ذلك بيانات الحكومة الاتحادية والحكومات المحلية والهيئات العامة والمؤسسات العامة الاتحادية والمحلية.

المادة (2):

1 ــ كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

2 ــ فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين.

3 ــ فإذا كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرة آلاف درهم أو بإحدى هاتين العقوبتين.

المادة (3):

كل من ارتكب أياً من الجرائم المنصوص عليها في البند (2) من المادة (2) من هذا القانون أثناء أو بسبب تأدية عمله أو سهل ذلك للغير يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرين ألف درهم أو بإحدى هاتين العقوبتين.

المادة (4):

يعاقب بالسجن المؤقت كل من زور مستنداً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفاً به قانوناً في نظام معلوماتي.
وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر.
ويعاقب بالعقوبة المقررة لجريمة التزوير حسب الأحوال من استعمل المستند المزور مع علمه بتزويره.

المادة (5):

كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

المادة (6):

كل من أدخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات فيها يعاقب بالسجن المؤقت وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين.

المادة (7):

يعاقب بالسجن المؤقت أو الحبس كل من عدل أو أتلف الفحوص الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو سهل للغير فعل ذلك، أو مكنه منه، باستعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

المادة (8):

كل من تنصت أو التقط أو اعترض عمداً، من دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

المادة (9):

كل من استعمل الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في تهديد أو ابتزاز شخص آخر لحمله على القيام بالفعل أو الامتناع عنه يعاقب بالحبس مدة لا تزيد على سنتين وبالغرامة التي لا تزيد على خمسين ألف درهم أو بإحدى هاتين العقوبتين، فإن كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف، أو الاعتبار كانت العقوبة السجن مدة لا تزيد على عشر سنوات

المادة (10):

كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ثلاثين ألفاً أو بإحدى هاتين العقوبتين.

المادة (11):

كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول من دون وجه حق، إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الالكترونية يعاقب بالحبس وبالغرامة فإن قصد من ذلك استخدامها في الحصول على أموال الغير، أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل ثلاثين ألف درهم أو إحدى هاتين العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير.

المادة (12):

كل من أنتج أو أعد أو هيأ أو أرسل أو خزن بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه المساس بالآداب العامة أو أدار مكاناً لذلك، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين. فإذا كان الفعل موجهاً إلى حدث فتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة لا تقل عن ثلاثين ألف درهم.

المادة (13):

يعاقب بالسجن وبالغرامة من حرض ذكراً أو أنثى أو أغواه لارتكاب الدعارة أو الفجور أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. فإن كان المجني عليه حدثاً كانت العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة.

المادة (14):

كل من دخل، من دون وجه حق، موقعاً في الشبكة المعلوماتية، لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

المادة (15):

يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، كل من ارتكب إحدى الجرائم التالية عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات:

-الإساءة إلى أحد المقدسات أو الشعائر الإسلامية.

-الإساءة إلى أحد المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقاً لأحكام الشريعة الإسلامية.

-سب أحد الأديان السماوية المعترف بها .

-حسن المعاصي أو حض عليها أو روج لها.

وتكون العقوبة السجن مدة لا تزيد على سبع سنوات إذا تضمنت الجريمة مناهضة للدين الإسلامي أو جرحاً للأسس والمبادئ التي يقوم عليها، أو ناهض أو جرح ما علم من الدين الإسلامي بالضرورة، أو نال من الدين الإسلامي، أو بشر بغيره أو دعا إلى مذهب أو فكرة تنطوي على شيء مما تقدم أو حبذ لذلك أو روج لها.

المادة (16):

كل من اعتدى على أي من المبادئ أو القيم الأسرية أو نشر أخباراً أو صوراً تتصل بحرمة الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين.

المادة (17):

كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الاتجار في الأشخاص أو تسهيل التعامل فيه، يعاقب بالسجن المؤقت.

المادة (18):

كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد ترويج المخدرات أو المؤثرات العقلية وما في حكمهما أو تسهيل التعامل فيهما وذلك في غير الأحوال المصرح بها قانوناً، يعاقب بالسجن المؤقت.

المادة (19):

مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال، يعاقب بالحبس مدة لا تزيد على سبع سنوات، وبالغرامة التي لا تقل عن ثلاثين ألفاً ولا تزيد على مائتي ألف درهم، كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام أو
اكتساب وحيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعاً لارتكاب أي من هذه الأفعال.

المادة (20):

كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة يعاقب بالحبس مدة لا تزيد على خمس سنوات.

المادة (21):
كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد على خمس سنوات.

المادة (22):

يعاقب بالسجن كل من دخل وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك.
فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها، تكون العقوبة السجن مدة لا تقل عن خمس سنوات.
ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

المادة (23)

كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها.

المادة (24):

مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكه، وذلك إغلاقاً كلياً أو للمدة التي تقدرها المحكمة.

المادة (25):

فضلاً عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالحبس وفقاً لأحكام هذا القانون.

المادة (26):

لا يخل تطبيق العقوبات المنصوص عليها في هذا القانون بأي عقوبة أشد ينص عليها في قانون العقوبات أو أي قانون آخر.

المادة (27)

تكون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل والشؤون الإسلامية والأوقاف صفة مأموري الضبط القضائي في ضبط الجرائم والمخالفات التي تقع بالمخالفة لأحكام هذا القانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم.

أحكام ختامية

المادة (28)

يلغى كل نص يخالف أحكام هذا القانون

المادة (29)

ينشر هذا القانون في الجريدة الرسمية ويعمل به اعتبارا من تاريخ نشره..

ملحق خاص بالقانون التونسي المتعلق بالمبادلات والتجارة الإلكترونية

الصادر في 9 أوت 2000م

القانون عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000
المتعلق بالمبادلات والتجارة الإلكترونية

باسم الشعب،

وبعد موافقة مجلس النواب،

يصدر رئيس الجمهورية القانون الآتي نصه :

الباب الأول
أحكام عامة

الفصل الأول : يضبط هذا القانون القواعد العامة المنظمة للمبادلات والتجارة الالكترونية.

وتخضع المبادلات والتجارة الالكترونية في ما لا يتعارض وأحكام هذا القانون إلى التشريع والتراتيب الجاري بها العمل.

يجري على العقود الالكترونية نظام العقود الكتابية من حيث التعبير عن الإرادة ومفعولها القانوني وصحتها وقابليتها للتنفيذ في ما لا يتعارض وأحكام هذا القانون.

الفصل 2 : يقصد في مفهوم هذا القانون بـــ:

-المبادلات الالكترونية: المبادلات التي تتم باستعمال الوثائق الالكترونية.

-التجارة الالكترونية: العمليات التجارية التي تتم عبر المبادلات الالكترونية.

-شهادة المصادقة الالكترونية: الوثيقة الالكترونية المؤمنة بواسطة الإمضاء الالكتروني للشخص الذي أصدرها والذي يشهد من خلالها، اثر المعاينة، على صحة البيانات التي تتضمنها.

-مزود خدمات المصادقة الالكترونية: كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الالكتروني.

-التشفير: إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو اشارات لا يمكن الوصول إلى المعلومة بدونها.

-منظومة إحداث الإمضاء :مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات المهيأة خصيصا لإحداث إمضاء الكتروني.

-منظومة التدقيق في الإمضاء: مجموعة من عناصر التشفير العمومية أو مجموعة من المعدات التي تمكن من التدقيق في الإمضاء الالكتروني.

-وسيلة الدفع الالكتروني: الوسيلة التي تمكن صاحبها من القيام بعمليات الدفع المباشر عن بعد عبر الشبكات العمومية للاتصالات.

-منتوج : كل خدمة أو منتوج طبيعي أو فلاحي أو جرفي أو صناعي، مادي أو لا مادي .

الفصل 3 : يخضع استعمال التشفير في المبادلات والتجارة الالكترونية عبر الشبكات العمومية للاتصالات إلى التراتيب الجاري بها العمل في ميدان الخدمات ذات القيمة المضافة للاتصالات.

الباب الثاني
في الوثيقة الالكترونية والإمضاء الالكتروني

الفصل 4 : يعتمد قانونا حفظ الوثيقة الالكترونية كما يعتمد حفظ الوثيقة الكتابية.
ويلتزم المرسل بحفظ الوثيقة الالكترونية في الشكل المرسلة به، ويلتزم المرسل إليه بحفظ هذه الوثيقة في الشكل الذي تسلمها به.
ويتم حفظ الوثيقة الالكترونية على حامل الكتروني يمكن من:
-الاطلاع على محتواها طيلة مدة صلوحيتها،
-حفظها في شكلها النهائي بصفة تضمن سلامة محتواها،
-حفظ المعلومات الخاصة بمصدرها ووجهتها وكذلك تاريخ ومكان إرسالها أو استلامها.

الفصل 5: يمكن لكل من يرغب في إمضاء وثيقة الكترونية إحداث إمضائه الالكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلف بالاتصالات.

الفصل 6 : يتعين على كل من يستعمل منظومة إمضاء الكتروني:
-اتخاذ الاحتياطات الدنيا التي يتم ضبطها في القرار المنصوص عليه بالفصل 5 من هذا القانون لتفادي كل استعمال غير مشروع لعناصر التشفير أو المعدات الشخصية المتعلقة بإمضائه،
-إعلام مزود خدمات المصادقة الالكترونية بكل استعمال غير مشروع لإمضائه،
-الحرص على مصداقية كافة المعطيات التي صرح بها لمزود خدمات المصادقة الالكترونية ولكافة الأطراف التي طلب منها أن تثق في إمضائه.

الفصل 7 : في صورة إخلاله بالالتزامات المنصوص عليها بالفصل 6 من هذا القانون، يتحمل صاحب الإمضاء مسؤولية الأضرار اللاحقة بالغير الناتجة عن ذلك.

الباب الثالث
في الوكالة الوطنية للمصادقة الالكترونية

الفصل 8 : أحدثت مؤسسة عمومية لا تكتسي صبغة إدارية تتمتع بالشخصية المعنوية وبالاستقلال المالي أطلق عليها اسم "الوكالة الوطنية للمصادقة الالكترونية" وتخضع في علاقاتها مع الغير إلى التشريع التجاري، ومقرها

بتونس العاصمة.

الفصل 9 : تتولى هذه المؤسسة القيام خاصة بالمهام التالية:

-منح ترخيص تعاطي نشاط مزود خدمات المصادقة الالكترونية على كامل تراب الجمهورية التونسية.

-السهر على مراقبة احترام مزود خدمات المصادقة الالكترونية لأحكام هذا القانون ونصوصه التطبيقية،

-تحديد مواصفات منظومة إحداث الإمضاء والتدقيق،

-إبرام اتفاقيات الاعتراف المتبادل مع الأطراف الأجنبية،

-إصدار وتسليم وحفظ شهادات المصادقة الالكترونية الخاصة بالأعوان العموميين المؤهلين للقيام بالمبادلات الالكترونية ويمكن أن يتم ذلك مباشرة أو عبر مزودي خدمات مصادقة الكترونية عموميين.

-المساهمة في أنشطة البحث والتكوين والدراسة ذات العلاقة بالمبادلات والتجارة الالكترونية.

وبصفة عامة كل نشاط آخر يقع تكليفها به من قبل سلطة الإشراف وله علاقة بميدان تدخلها.

وهي تخضع لإشراف الوزارة المكلفة بالقطاع.

الفصل10: يمكن أن تسند إلى الوكالة الوطنية للمصادقة الالكترونية عن طريق التخصيص ممتلكات الدولة المنقولة وغير المنقولة الضرورية للقيام بمهامها. وفي صورة حل المؤسسة ترجع ممتلكاتها إلى الدولة التي تتولى تنفيذ التزاماتها وتعهداتها طبقا للتشريع الجاري به العمل.

الباب الرابع
في خدمات المصادقة الالكترونية

الفصل11: يتعين على كل شخص طبيعي أو معنوي يرغب في تعاطي نشاط مزود خدمات المصادقة الالكترونية الحصول على ترخيص مسبق من الوكالة الوطنية للمصادقة الالكترونية.

ويجب أن تتوفر في الشخص الطبيعي أو الممثل القانوني للشخص المعنوي الراغب في الحصول على ترخيص لتعاطي نشاط مزود خدمات المصادقة الالكترونية الشروط التالية:

-أن يكون من ذوي الجنسية التونسية منذ خمسة أعوام على الأقل،

-أن يكون مقيما بالبلاد التونسية،

-أن يكون متمتعا بحقوقه المدنية والسياسية ونقي السوابق العدلية،

-أن يكون متحصلا على الأقل على شهادة الأستاذية أو ما يعادلها،

-أن لا يتعاطى نشاطا مهنيا آخر،

الفصل 12 : يتولى كل مزود خدمات المصادقة الالكترونية إصدار وتسليم وحفظ الشهادات وفقا لكراس شروط تتم المصادقة عليه بأمر، وعند الاقتضاء تعليقها أو إلغاءها وفقا لأحكام هذا القانون.

ويتضمن كراس الشروط خاصة:

-كلفة دراسة ومتابعة ملفات مطالب الشهادات،
-آجال دراسة الملفات،
-الإمكانيات المادية والمالية والبشرية التي يجب توفرها لتعاطي النشاط،
-شروط تأمين التفاعل المتبادل لأنظمة المصادقة وربط سجلات شهادات المصادقة،
-القواعد المتعلقة بالإعلام والخاصة بخدماته والشهادات التي سلمها والتي يتعين على مزود خدمات المصادقة الالكترونية حفظها.

الفصل 13: يتعين على مزود خدمات المصادقة الالكترونية استعمال وسائل موثوق بها لإصدار وتسليم وحفظ الشهادات واتخاذ الوسائل اللازمة لحمايتها من التقليد والتدليس وفقا لكراس الشروط المنصوص عليه بالفصل 12 من هذا القانون.

الفصل 14: على كل مزود خدمات مصادقة الكترونية مسك سجل الكتروني لشهادات المصادقة على ذمة المستعملين مفتوح للاطلاع الكترونيا بصفة مستمرة على المعلومات المدونة به.
ويتضمن سجل شهادات المصادقة، عند الاقتضاء تاريخ تعليق الشهادات أو إلغاءها.
ويتعين حماية هذا السجل وشهادة المصادقة من كل تغيير غير مرخص فيه.

الفصل 15: يتعين على مزودي خدمات المصادقة الالكترونية وأعوانهم المحافظة على سرية المعلومات التي عهدت إليهم في إطار تعاطي أنشطتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل.

الفصل 16: يتولى مزود خدمات المصادقة الالكترونية، عند طلب شهادة جمع المعلومات ذات الصبغة الشخصية مباشرة من الشخص المعني وله أن يتحصل عليها من الغير بعد الموافقة الكتابية أو الالكترونية لهذا الشخص.
يحجر على مزود خدمات المصادقة الالكترونية جمع المعلومات التي لا تكون ضرورية لتسليم الشهادة.
ويحجر عليه استعمال المعلومات التي جمعها بغرض تسليم الشهادة خارج إطار أنشطة المصادقة، ما لم يحصل كتابيا أو الكترونيا على موافقة الشخص المعني .

الفصل 17: يصدر مزود خدمات المصادقة الالكترونية شهادات مصادقة تستجيب لمقتضيات السلامة والوثوق بها.
وتضبط المعطيات التقنية المتعلقة بالشهادة والوثوق بها بقرار من الوزير المكلف بالاتصالات.
وتتضمن هذه الشهادة بالخصوص:
-هوية صاحب الشهادة،
-هوية الشخص الذي أصدرها وإمضائه الالكتروني،
-عناصر التدقيق في إمضاء صاحب الشهادة.
-مدة صلوحية الشهادة،

-مجالات استعمال الشهادة.

الفصل 18: يضمن مزود خدمات المصادقة الالكترونية:
-صحة المعلومة المصادقة عليها التي تضمنتها الشهادة في تاريخ تسليمها،
-الصلة بين صاحب الشهادة ومنظومة التدقيق في الإمضاء الخاصة به،
-انفراد صاحب الشهادة بمسك منظومة إحداث إمضاء مطابقة لأحكام القرار المنصوص عليه بالفصل 5 من هذا القانون ومتكاملة مع منظومة التدقيق في الإمضاء المعرفة في الشهادة في تاريخ تسلمها،
وعند تسليم شهادة المصادقة إلى شخص معنوي يتعين على مزود خدمات المصادقة الالكترونية التدقيق مسبقا في هوية الشخص الطبيعي الذي يتقدم إليه وصفة تمثيله للشخص المعنوي.

الفصل 19: يتولى مزود خدمات المصادقة الالكترونية تعليق العمل بشهادة المصادقة حالا بطلب من صاحبها او عندما يتبين:
-أن الشهادة سلمت بالاعتماد على معلومات مغلوطة أو مزيفة،
-انه تم انتهاك منظومة إحداث الإمضاء،
-أن الشهادة استعملت بغرض التدليس،
-أن المعلومات المضمنة بالشهادة قد تغيرت.
ويتولى مزود خدمات المصادقة الالكترونية إعلام صاحب الشهادة حالا بالتعليق وسببه.
ويتم رفع هذا التعليق حالا إذا تبينت صحة المعلومات المدونة بالشهادة واستعمالها بصفة شرعية.
ويعارض صاحب الشهادة أو الغير بقرار مزود الخدمات الخاص بتعليق الشهادة من تاريخ نشره بالسجل الالكتروني المنصوص عليه بالفصل 14 من هذا القانون.

الفصل 20 : يلغي مزود خدمات المصادقة الالكترونية حالا الشهادة في الحالات التالية:
-عند طلب صاحب الشهادة،
-عند إعلامه بوفاة الشخص الطبيعي أو انحلال الشخص المعنوي صاحب الشهادة،
-عند القيام باختبارات دقيقة، بعد تعليقها، تبين أن المعلومات مغلوطة أو مزيفة أو أنها غير مطابقة للواقع أو انه قد تم انتهاك منظومة إحداث الإمضاء أو الاستعمال المدلس للشهادة.
ويعارض صاحب الشهادة أو الغير بقرار مزود الخدمات الخاص بإلغاء الشهادة من تاريخ نشره بالسجل الالكتروني المنصوص عليه بالفصل 14 من هذا القانون.

الفصل 21 : يكون صاحب الشهادة المسؤول الوحيد عن سرية وسلامة منظومة إحداث الإمضاء التي يستعملها، وكل استعمال لهذه المنظومة يعتبر صادرا منه.
ويتعين على صاحب الشهادة إعلام مزود خدمات المصادقة الالكترونية بكل تغيير للمعلومات المضمنة بالشهادة.
لا يمكن لصاحب الشهادة التي تم تعليقها أو إلغاؤها استعمال عناصر التشفير الشخصية للإمضاء موضوع الشهادة

المعنية والمصادقة على هذه العناصر من جديد لدى مزود آخر لخدمات المصادقة الالكترونية.

الفصل 22 : يكون مزود خدمات المصادقة الالكترونية مسؤولا عن كل ضرر حصل لشخص وثق عن حسن نية في الضمانات المنصوص عليها بالفصل 18 من هذا القانون.
ويكون مزود خدمات المصادقة الالكترونية مسؤولا عن الضرر الحاصل لكل شخص نتيجة عدم تعليق أو إلغاء شهادة طبقا للفصلين 19 و20 من هذا القانون.
لا يكون مزود خدمات المصادقة الالكترونية مسؤولا عن الضرر الناتج عن عدم احترام صاحب الشهادة لشروط استعمالها أو شروط إحداث إمضائه الالكتروني.

الفصل 23 : تعتبر الشهادات المسلمة من مزود خدمات المصادقة الإلكترونية الموجود ببلد أجنبي كشهادات مسلمة من مزود خدمات المصادقة الالكترونية موجود بالبلاد التونسية إذا تم الاعتراف بهذا الهيكل في إطار اتفاقية اعتراف متبادل تبرمها الوكالة الوطنية للمصادقة الالكترونية.

الفصل 24 : يتعين على مزود خدمات المصادقة الالكترونية الراغب في إيقاف نشاطه إعلام الوكالة الوطنية للمصادقة الالكترونية قبل تاريخ الإيقاف بثلاثة أشهر على الأقل.
ويمكن لمزود خدمات المصادقة الالكترونية تحويل جزء أو كل نشاطه إلى مزود آخر، ويتم هذا التحويل حسب الشروط التالية:
-إعلام أصحاب الشهادات الجاري بها العمل برغبته في تحويل الشهادات إلى مزود آخر قبل شهر من التحويل المنتظر على الأقل،
-تحديد هوية مزود خدمات المصادقة الالكترونية الذي ستحول إليه الشهادات،
-إعلام أصحاب الشهادات بإمكانية رفض التحويل المنتظر وكذلك أجال وطرق الرفض. وتلغى الشهادات إذا عبر أصحابها كتابيا أو الكترونيا عن رفضهم في هذا الأجل.
وفي حالة وفاة أو إفلاس أو حل أو تصفية مزود خدمات المصادقة الالكترونية يخضع ورثته أو وكلاؤه أو المصفون إلى مقتضيات الفقرة الثانية من هذا الفصل في أجل لا يتجاوز ثلاثة أشهر.
وفي كل حالات إيقاف النشاط يتعين إتلاف المعطيات الشخصية التي بقيت تحت تصرف المزود وذلك بحضور ممثل عن الوكالة الوطنية للمصادقة الالكترونية.

الباب الخامس
في المعاملات التجارية الإلكترونية

الفصل 25: يجب على البائع، في المعاملات التجارية الالكترونية، أن يوفر للمستهلك بطريقة واضحة ومفهومة، قبل إبرام العقد المعلومات التالية:
-هوية وعنوان وهاتف البائع أو مسدي الخدمات،
-وصفا كاملا لمختلف مراحل انجاز المعاملة،
-طبيعة وخاصيات وسعر المنتوج،

-كلفة تسليم المنتوج ومبلغ تأمينه والاداءات المستوجبة،
-الفترة التي يكون خلالها المنتوج معروضا بالأسعار المحددة،
-شروط الضمانات التجارية والخدمة بعد البيع،
-طرق وإجراءات الدفع، وعند الاقتضاء شروط القروض المقترحة،
-طرق وأجال التسليم وتنفيذ العقد ونتائج عدم انجاز الالتزامات،
-إمكانية العدول عن الشراء وأجله،
-كيفية إقرار الطلبية،
-طرق إرجاع المنتوج أو الإبدال وإرجاع المبلغ،
-كلفة استعمال تقنيات الاتصالات حين يتم احتسابها على أساس مختلف عن التعريفات الجاري بها العمل،
-شروط فسخ العقد إذا كان لمدة غير محددة أو تفوق السنة،
-المدة الدنيا للعقد، في ما يخص العقود المتعلقة بتزويد المستهلك بمنتوج أو خدمة خلال مدة طويلة أو بصفة دورية،
يتعين توفير هذه المعلومات الكترونيا ووضعها على ذمة المستهلك للإطلاع عليها في جميع مراحل المعاملة.

الفصل 26: يحجر على البائع تسليم منتوج مشروط بطلب دفع، لم تصدر بشأنه طلبية من قبل المستهلك.
وفي حالة تسليم منتوج إلى المستهلك لم تصدر بشأنه طلبية، لا يمكن مطالبة هذا الأخير بسعره أو كلفة تسليمه.

الفصل 27: يتعين على البائع، قبل إبرام العقد، تمكين المستهلك من المراجعة النهائية لجميع اختياراته وتمكينه من إقرار الطلبية أو تغييرها حسب إرادته، وكذلك الاطلاع على شهادة المصادقة الالكترونية المتعلقة بإمضائه.

الفصل 28 : ينشأ العقد الالكتروني بعنوان البائع وفي تاريخ موافقة هذا الأخير على الطلبية بواسطة وثيقة الكترونية ممضاة وموجهة للمستهلك، ما لم يتفق الطرفان على خلاف ذلك.

الفصل 29: يتعين على البائع أن يوفر إلى المستهلك، عند الطلب، خلال العشرة أيام الموالية لإبرام العقد وثيقة كتابية أو الكترونية تتضمن كافة المعطيات المتعلقة بعملية البيع.

الفصل 30: مع مراعاة مقتضيات الفصل 25 من هذا القانون، يمكن للمستهلك العدول عن الشراء في أجل عشرة أيام عمل، تحتسب:
-بالنسبة إلى البضائع بداية من تاريخ تسلمها من قبل المستهلك،
-بالنسبة إلى الخدمات بداية من تاريخ إبرام العقد.
ويتم الإعلام بالعدول بواسطة جميع الوسائل المنصوص عليها مسبقا في العقد.
في هذه الحالة، يتعين على البائع إرجاع المبلغ المدفوع إلى المستهلك في أجل عشرة أيام عمل من تاريخ إرجاع البضاعة أو العدول عن الخدمة.
ويتحمل المستهلك المصاريف الناجمة عن إرجاع البضاعة.

الفصل 31: بقطع النظر عن جبر الضرر لفائدة المستهلك، يمكن لهذا الأخير إرجاع المنتوج على حالته اذا كان غير مطابق للطلبية أو إذا لم يحترم البائع أجال تسليمه وذلك في اجل عشرة أيام عمل تحتسب بداية من تاريخ التسليم.

في هذه الحالة، يتعين علي البائع إرجاع المبلغ المدفوع والمصاريف الناجمة عن ذلك إلى المستهلك في أجل عشرة أيام عمل من تاريخ إرجاع المنتوج.

الفصل 32 : مع مراعاة أحكام الفصل 30 من هذا القانون وباستثناء حالات العيوب الظاهرة أو الخفية، لا يمكن للمستهلك العدول عن الشراء في الحالات التالية:

-عندما يطلب المستهلك توفير الخدمة قبل انتهاء اجل العدول عن الشراء ويوفر البائع ذلك،

-إذا تم تزويد المستهلك بمنتوجات حسب خاصيات شخصية أو تزويده بمنتوجات لا يمكن إعادة إرسالها أو تكون قابلة للتلف أو الفساد لانتهاء مدة صلوحيتها،

-عند قيام المستهلك بنزع الأختام عن التسجيلات السمعية أو البصرية أو البرمجيات والمعطيات الإعلامية المسلمة أو نقلها آليا،

-شراء الصحف والمجلات.

الفصل 33 : إذا كانت عملية الشراء ناتجة كليا أو جزئيا عن قرض ممنوح إلى المستهلك من قبل البائع أو الغير على أساس عقد مبرم بين هذا الأخير والغير، فإن عدول المستهلك عن الشراء يفسخ عقد القرض بدون تعويض.

الفصل 34: باستثناء حالات سوء الاستعمال يتحمل البائع، في حالة البيع مع التجربة، الأخطار التي قد يتعرض إليها المنتوج وذلك إلى غاية انتهاء مدة تجربته. ويعد لاغيا كل شرط للإعفاء من المسؤولية يكون مخالفا لأحكام هذا الفصل.

الفصل 35 : يتعين على البائع، في صورة عدم توفر المنتوج أو الخدمة المطلوبة إعلام المستهلك بذلك في أجل أقصاه 24 ساعة قبل تاريخ التسليم المنصوص عليه في العقد وإرجاع كامل المبلغ المدفوع إلى صاحبه.

وباستثناء حالات القوة القاهرة، يفسخ العقد إذا أخل البائع بالتزاماته، ويسترجع المستهلك المبلغ المدفوع بقطع النظر عن جبر الضرر اللاحق به.

الفصل 36: على البائع إثبات حصول الإعلام المسبق وإقرار المعلومات واحترام الآجال وقبول المستهلك وكل اتفاق مخالف يعد باطلا.

الفصل 37: تخضع عمليات الدفع المتعلقة بالمبادلات والتجارة الالكترونية إلى التشريع والتراتيب الجاري بها العمل.

يجب على صاحب وسيلة الدفع الالكتروني إعلام مصدرها بضياعها أو سرقتها أو ضياع أو سرقة الوسائل التي تمكن من استعمالها وكذلك كل استعمال مزيف لها.

يجب على مصدر وسيلة الدفع الالكتروني تحديد الوسائل الملائمة لهذا الإعلام في العقد المبرم مع صاحبها.
بقطع النظر عن حالات التدليس، فان صاحب وسيلة الدفع الالكتروني:
-يتحمل، إلى تاريخ إعلامه المصدر، نتائج ضياع أو سرقة وسيلة الدفع أو استعمالها المزيف من قبل الغير،
-لا يتحمل أي مسؤولية من استعمال وسيلة الدفع الالكتروني بعد إعلام المصدر.
واستعمال وسيلة الدفع الالكتروني دون تقديم الوسيلة وتحديد الهوية الكترونيا لا يلزم صاحبها.

الباب السادس
في حماية المعطيات الشخصية

الفصل 38: لا يمكن لمزود خدمات المصادقة الالكترونية معالجة المعطيات الشخصية إلا بعد موافقة صاحب الشهادة المعني.
ويمكن اعتماد الإعلام الالكتروني بالموافقة إذا ضمن المزود:
-إعلام صاحب الشهادة بحقه في سحب الموافقة في كل وقت،
-إمكانية تحديد هوية الأطراف المستعملة للمعطيات الشخصية،
-الاحتفاظ بحجة الموافقة التي لا يمكن تغييرها.

الفصل 39 : باستثناء حالة موافقة صاحب الشهادة، لا يمكن لمزود خدمات المصادقة الالكترونية أو احد أعوانه جمع المعلومات الخاصة بصاحب الشهادة إلا ما كان منها ضروريا لإبرام العقد وتحديد محتواه وتنفيذه وإعداد وإصدار الفاتورة.
لا يمكن استعمال المعطيات المجمعة طبقا للفقرة الأولى من هذا الفصل لغير الغاية المذكورة أعلاه من قبل المزود أو غيره إلا إذا تم إعلام صاحب الشهادة بذلك ولم يعارضه.

الفصل 40: يمنع على مستعملي المعطيات الشخصية المجمعة طبقا للفصل 39 من هذا القانون إرسال الوثائق الإلكترونية إلى صاحب الشهادة الذي يرفض صراحة قبولها.
ويتعين على صاحب الشهادة إعلام الوكالة الوطنية للمصادقة الإلكترونية باعتراضه بواسطة رسالة مضمونة الوصول مع إعلام بالبلوغ.
ويعتبر هذا الإعلام قرينة قاطعة علي معرفة كل المزودين والغير لهذا الاعتراض.

الفصل 41 : يتعين على مزود خدمات المصادقة الالكترونية، قبل كل معالجة للمعلومات الشخصية، إعلام صاحب الشهادة بواسطة إشعار خاص بالإجراءات المتبعة من قبله في مجال حماية المعطيات الشخصية. ويتعين أن تمكن هذه الإجراءات صاحب الشهادة من الاطلاع آليا وبطريقة مبسطة على محتوى المعطيات.
ويجب أن تحدد هذه الإجراءات هوية المسؤول عن المعالجة وطبيعة المعطيات والغاية من المعالجة وأصناف وأماكن المعالجة، وعند الاقتضاء كل معلومة ضرورية لضمان المعالجة الأمينة للمعطيات.

الفصل 42 : يمكن لصاحب الشهادة، في كل وقت، بطلب ممضى بخط اليد أو الكترونيا النفاذ إلى المعلومات الشخصية المتعلقة به وتعديلها. ويشمل حق النفاذ والتعديل الدخول على جميع المعطيات الشخصية المتعلقة بصاحب الشهادة.

ويتعين على المزود وضع الإمكانيات التقنية اللازمة لتمكين صاحب الشهادة من إرسال مطلبه الممضى لتعديل المعلومات او فسخها بطريقة الكترونية.

الباب السابع

في المخالفات والعقوبات

الفصل 43 : تتم معاينة المخالفات لأحكام هذا القانون من قبل أعوان الضابطة العدلية والأعوان المحلفين للوزارة المكلفة بالاتصالات والوكالة الوطنية للمصادقة الالكترونية وأعوان المراقبة الاقتصادية وفق الشروط المنصوص عليها بالقانون عدد 64 لسنة 1991 المؤرخ في 29 جويلية 1991 المتعلق بالمنافسة والأسعار والنصوص المنقحة والمتممة له.

الفصل 44 : يسحب الترخيص من مزود خدمات المصادقة الالكترونية ويتم إيقاف نشاطه، إذا أخل بواجباته المنصوص عليها بهذا القانون أو بنصوصه التطبيقية. وتتولى الوكالة الوطنية للمصادقة الالكترونية سحب الترخيص بعد سماع المزود المعني بالأمر.

الفصل 45 : علاوة على العقوبات المبينة بالفصل 44 من هذا القانون يعاقب كل مزود خدمات المصادقة الالكترونية لم يراع مقتضيات كراس الشروط المنصوص عليه بالفصل 12 من هذا القانون بخطية تتراوح بين 1.000 و10.000 دينار.

الفصل 46: يعاقب كل من يمارس نشاط مزود خدمات المصادقة الالكترونية بدون الحصول على ترخيص مسبق طبقا للفصل 11 من هذا القانون بالسجن لمدة تتراوح بين شهرين و3 سنوات وبخطية تتراوح بين 1.000 و10.000 دينار أو بإحدى هاتين العقوبتين.

الفصل 47 : يعاقب كل من صرح عمدا بمعطيات خاطئة لمزود خدمات المصادقة الالكترونية ولكافة الأطراف التي طلب منها أن تثق بإمضائه بالسجن لمدة تتراوح بين 6 أشهر وعامين وبخطية تتراوح بين 1.000 و10.000 دينار أو بإحدى هاتين العقوبتين.

الفصل 48: يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة

تتراوح بين 6 أشهر وعامين وبخطية تتراوح بين 1.000 و10.000 دينار أو بإحدى هاتين العقوبتين.

الفصل 49 : يعاقب كل مخالف لأحكام الفصول 25 و27 و29 والفقرة الثانية من الفصل 31 والفصل 34 والفقرة الأولى من الفصل 35 من هذا القانون بخطية تتراوح بين 500 و5.000 دينار.

الفصل 50 : يعاقب كل من استغل ضعف أو جهل شخص في إطار عمليات البيع الالكتروني بدفعه الالتزام حاضرا أو آجلا بأي شكل من الأشكال، بخطية تتراوح بين 1.000 و20.000 دينار، وذلك إذا ثبت من ظروف الواقعة أن هذا الشخص غير قادر على تمييز أبعاد تعهداته أو كشف الحيل والخدع المعتمدة بالالتزام أو إذا ثبت انه كان تحت الضغط، مع مراعاة أحكام المجلة الجنائية.

الفصل 51: يعاقب كل مخالف لأحكام الفصلين 38 و39 بخطية تتراوح بين 1000 و10000 دينار.

الفصل 52 : يعاقب طبقا لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الالكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل.

الفصل 53: مع حفظ الحقوق المدنية للمتضررين، يمكن للوزير المكلف بالتجارة إجراء الصلح في المخالفات المنصوص عليها بالفصل 49 من هذا القانون والتي تتم معاينتها وفقا لأحكام هذا القانون.
مع حفظ الحقوق المدنية للمتضررين، يمكن للوزير المشرف على الوكالة الوطنية للمصادقة الالكترونية إجراء الصلح في المخالفات المنصوص عليها بالفصل 45 من هذا القانون والتي تتم معاينتها وفقا لأحكام هذا القانون.
وتكون طرق وإجراءات الصلح وفق النصوص القانونية الجاري بها العمل والمنظمة للمراقبة الاقتصادية وخاصة القانون عدد 64 لسنة 1991 المؤرخ في 29 جويلية 1991 المتعلق بالمنافسة والأسعار والنصوص المنقحة والمتممة له، بدون المساس بحقوق الغير.
تنقرض الدعوى العمومية بدفع المبلغ المعين في عقد الصلح.
ينشر هذا القانون بالرائد الرسمي للجمهورية التونسية وينفذ كقانون من قوانين الدولة.

تونس في 9 أوت 2000

زين العابدين بن علي

ملحق خاص بالقانون الجزائري المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

الصادر في 05 أوت 2009م

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة

الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات عملية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني
مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إنابة لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث
القواعد الإجرائية
تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

ملحق خاص ببنود اتفاقية بودابيست حول الجريمة الإلكترونية

المنعقدة في 23 نوفمبر 2001

Convention on Cybercrime

Budapest, 23.11.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom

to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system,

including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2

through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the

execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on

international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the

requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article

14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or

any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

ملحق خاص بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات

21 ديسمبر 2010

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الديباجة :

إن الدول العربية الموقعة،

رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها،

واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات،

وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة،

والتزاماً بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها،

فقد اتفقت على ما يلي:

الفصل الأول

أحكام عامة

المادة الأولى: الهدف من الاتفاقية:

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المادة الثانية: المصطلحات:

يقصد بالمصطلحات التالية في هذه الاتفاقية التعريف المبين إزاء كل منها:

1- **تقنية المعلومات:** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة.

2- **مزود الخدمة:** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.

3- **البيانات :** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها...

4- **البرنامج المعلوماتي:** مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.
5- **النظام المعلوماتي:** مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.
6- **الشبكة المعلوماتية:** ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.
7- **الموقـــع :** مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.
8- **الالتقـــاط :** مشاهدة البيانات أو المعلومات أو الحصول عليها.
9- **معلومات المشترك:** أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:
أ - نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.
ب- هويـــة المشـــترك وعنوانـــه البريـــدي أو الجغرافـــي أو هاتفـــه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.
ج - أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.

المادة الثالثة: مجالات تطبيق الاتفاقية:

تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية :

1 – ارتكبت في أكثر من دولة.
2- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.
3- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.
4- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

المادة الرابعة: صون السيادة:

1- تلتزم كل دولة طرف وفقاً لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.
2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

الفصل الثاني

التجريم

المادة الخامسة: التجريم:

تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية.

المادة السادسة: جريمة الدخول غير المشروع:

1- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
2- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:
أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.
ب- الحصول على معلومات حكومية سرية.

المادة السابعة: جريمة الاعتراض غير المشروع:

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

المادة الثامنة: الاعتداء على سلامة البيانات:

1- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.
2- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم.

المادة التاسعة: جريمة إساءة استخدام وسائل تقنية المعلومات:

1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ - أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب- كلمة سر نظام معلومات أو شيفرة دخول او معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

المادة العاشرة: جريمة التزوير:

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

المادة الحادية عشرة: جريمة الاحتيال:

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:
1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.
2- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

3- تعطيل الأجهزة والبرامج والمواقع الالكترونية.

المادة الثانية عشرة: جريمة الإباحية:

1- انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.
2- تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.
3- يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

المادة الثالثة عشرة: الجرائم الأخرى المرتبطة بالإباحية:

المقامرة والاستغلال الجنسي.

المادة الرابعة عشرة: جريمة الاعتداء على حرمة الحياة الخاصة:

الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات .

المادة الخامسة عشرة: الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

المادة السادسة عشرة: الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات:

1- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.
2- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.
3- الاتجار بالأشخاص.
4- الاتجار بالأعضاء البشرية.
5- الاتجار غير المشروع بالأسلحة.

المادة السابعة عشرة: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة:

انتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي.

المادة الثامنة عشرة: الاستخدام غير المشروع لأدوات الدفع الالكترونية:

1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.

2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.
3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.
4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

المادة التاسعة عشرة: الشروع والاشتراك في ارتكاب الجرائم:

1- الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف.
2- الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية.
3- يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كلياً أو جزئياً.

المادة العشرون: المسؤولية الجنائية للأشخاص الطبيعية والمعنوية:

تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصياً.

المادة الحادية والعشرون: تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

الفصل الثالث

الأحكام الإجرائية

المادة الثانية والعشرون: نطاق تطبيق الأحكام الإجرائية:

1- تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والاجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية.
2- مع مراعاة أحكام المادة التاسعة والعشرين، على كل دولة طرف تطبيق الصلاحيات والإجراءات المذكورة في الفقرة (1) على:
   أ- الجرائم المنصوص عليها في المواد السادسة إلى التاسعة عشرة من هذه الاتفاقية.
   ب- أية جرائم أخرى ترتكب بواسطة تقنية المعلومات.
   ج- جمع الأدلة عن الجرائم بشكل إلكتروني.
3- أ- يجوز لأي دولة طرف الاحتفاظ بحقها في تطبيق الإجراءات المذكورة في المادة التاسعة والعشرين فقط على الجرائم أو أصناف الجرائم المعنية في التحفظ بشرط أن لا

يزيد عدد هذه الجرائم على عدد الجرائم التي تطبق عليها الإجراءات المذكورة في المادة الثلاثين، وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادة التاسعة والعشرين.

ب- كما يجوز للدولة الطرف أن تحتفظ بحقها في عدم تطبيق تلك الإجراءات كلما كانت غير قادرة بسبب محدودية التشريع على تطبيقها على الاتصالات التي تبث بواسطة تقنية معلومات لمزود خدمة، وذلك إذا كانت التقنية:

- يتم تشغيلها لصالح مجموعة مغلقة من المستخدمين.
- لا تستخدم شبكات اتصال عامة وليست مرتبطةً بتقنية معلومات أخرى سواء كانت عامة أو خاصة.

وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادتين التاسعة والعشرين والثلاثين.

المادة الثالثة والعشرون: التحفظ العاجل على البيانات المخزنة في تقنية المعلومات:

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصاً إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوماً قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للابقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.

المادة الرابعة والعشرون: التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين:

تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل :

1 - ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات.

2- ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.

المادة الخامسة والعشرون: أمر تسليم المعلومات:

تلتزم كل دولة طرف بتبني الاجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى:

1 - أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.
2 - أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمه أو تحت سيطرته.

المادة السادسة والعشرون: تفتيش المعلومات المخزنة:

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:
أ - تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.
ب - بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.
2 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1 - أ) اذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

المادة السابعة والعشرون: ضبط المعلومات المخزنة:

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقره (1) من المادة السادسة والعشرين من هذه الاتفاقية .
هذه الإجراءات تشمل صلاحيات :
أ - ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.
ب - عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها .
ج - الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.
د - إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.
3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (2,1) من المادة السادسة والعشرين من هذه الاتفاقية.

المادة الثامنة والعشرون: الجمع الفوري لمعلومات تتبع المستخدمين:

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من:
أ - جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف.
ب - إلزام مزود الخدمة ضمن اختصاصة الفني بأن :

- يجمع أو يسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف،أو
- يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2 - إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقره (1 – أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3 - تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

المادة التاسعة والعشرون: إعتراض معلومات المحتوى :

1 - تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من:
أ - الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف، أو
ب - التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية معلومات .

2 - إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1 – أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3- تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

الفصل الرابع

التعاون القانوني والقضائي

المادة الثلاثون: الاختصاص :

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت:
أ - في إقليم الدولة الطرف.
ب- على متن سفينة تحمل علم الدولة الطرف.
ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

د- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

3- إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم.

المادة الحادية والثلاثون: تسليم المجرمين:

1- أ- هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الاطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.

ب- إذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق.

2- إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبر جرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف.

3- إذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة.

4- الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة (1) من هذه المادة قابلة لتسليم المجرمين بين تلك الدول.

5- يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها لرفض تسليم المجرمين.

6- يجوز لكل دولة طرف من الأطراف المتعاقدة أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة أو بعقوبة أشد لدى أي من الطرفين المتعاقدين وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلباً بالملاحقة مصحوبا بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازتها وتحاط الدولة الطرف الطالبة علما بما يتم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم.

7- أ- تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإيصال اسم وعنوان السلطة المسؤولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي في

ظل غياب معاهدة إيصال هذه المعلومات إلى الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب.

ب- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل السلطات المعنية من قبل الدول الأطراف وعلى كل دولة طرف أن تضمن أن تفاصيل السجل صحيحة دائماً.

المادة الثانية والثلاثون: المساعدة المتبادلة :

1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم.

2- تلتزم كل دولة طرف بتبنى الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين.

3- يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك إستخدام التشفير) وتأكيد الإرسال حسبما تطلب الدولة الطرف ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات.

4- باستثناء ما يرد فيه نص في هذا الفصل فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها أن تمارس حقها في رفض المساعدة فيما يتعلق بالجرائم المنصوص عليها في الفصل الثاني فقط بناء على كون الطلب يخص جريمة يعتبرها من الجرائم المالية.

5- حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فإن هذا الشرط يعتبر حاصلاً بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة وذلك إذا كان الفعل الذي يمهد للجريمة التي تطلب المساعدة فيها يعتبر جريمة بحسب قوانين الدولة الطرف.

المادة الثالثة والثلاثون: المعلومات العرضية المتلقاة :

1- يجوز لأي دولة طرف – ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف.

2- قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات, وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات، وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.

المادة الرابعة والثلاثون: الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة:

1- تطبق بنود الفقرات (2-9) من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطرف الطالبة والمطلوب منها، أما في حال وجودها فلا تطبق الفقرات المشار اليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي.

2- أ- على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها.

ب- على السلطات المركزية أن تتصل ببعضها مباشرة.

ج- على كل دولة طرف – وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة.

د- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائماً.

3- يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة.

4- يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها.

5- قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذا سيتم تلبية الطلب جزئياً أو يكون خاضعاً للشروط التي قد تراها ضرورية.

6- تلتزم الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب, وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير.

7- يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر الكافي لتنفيذ الطلب, وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب.

8- أ- في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها، وفي مثل هذه الحالات يجب إرسال نسخة في نفس الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها.

ب- يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول.

ج- حيثما يتم تقديم طلب حسب الفقرة(أ) ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك.

د- إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة.

هـ- يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الإنضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.

المادة الخامسة والثلاثون: رفض المساعدة:

يجوز للدولة الطرف المطلوب منها المساعدة - بالاضافة إلى أسس الرفض المنصوص عليها في المادة الثانية والثلاثين الفقرة (4) أن ترفض المساعدة إذا:

1- كان الطلب متعلقاً بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية.

2- اعتبر أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لسيادته أو أمنه أو نظامه أو مصالحه الأساسية.

المادة السادسة والثلاثون: السرية وحدود الاستخدام:

1- عندما لايكون هناك معاهدة أو اتفاق للمساعدة المتبادلة على أساس التشريع الساري بين الدول الأطراف الطالبة والمطلوب منها فيجب تطبيق بنود هذه المادة ولا يتم تطبيقها إذا وجدت مثل هذه الاتفاقية أو المعاهدة إلا إذا اتفقت الدول الأطراف المعنية على تطبيق أي من فقرات هذه المادة أو كلها.

2- يجوز للدولة الطرف المطلوب منها توفير المعلومات أو المواد الموجودة في الطلب بشرط:

أ - الحفاظ على عنصر السرية للدولة الطرف الطالبة للمساعدة ولا يتم الالتزام بالطلب في غياب هذا العنصر.

ب- عدم استخدام المعلومات في تحقيقات أخرى غير الواردة في الطلب.

3- إذا لم تستطع الدولة الطرف الطالبة الالتزام بالشرط الوارد في الفقرة (2) فيجب عليها إعلام الدولة الطرف الأخرى والتي ستقرر بعدها مدى إمكانية توفير المعلومات، وإذا قبلت الدولة الطرف الطالبة بهذا الشرط فهو ملزم لها.

4- أي دولة طرف توفر المعلومات أو المواد بحسب الشرط في الفقرة (2) لتوفير المعلومات يجوز لها أن تطلب من الدولة الطرف الأخرى أن تبرر استخدام المعلومات أو المواد.

المادة السابعة والثلاثون: الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات:

1- لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلباً بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

2- يجب أن يحدد طلب الحفظ حسب الفقرة (1) ما يلي:

أ- السلطة التي تطلب الحفظ.

ب- الجريمة موضوع التحقيق وملخصاً للوقائع.

ج- معلومات تقنية المعلومات التي يجب حفظها وعلاقتها بالجريمة.

د- أيـة معلومـات متـوفرة لتحديـد المسـؤول عـن المعلومـات المخزنـة أو موقـع تقنيـة المعلومات.

هـ- موجبات طلب الحفظ.

و- رغبة الدولة الطرف بتسليم طلب المساعدة الثنائية للبحث أو الوصـول أو الضبط أو تأمين أو كشف معلومات تقنية المعلومات المخزنة.

3- عند استلام إحدى الدول الأطراف الطلب من دولة طرف أخرى فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الاستجابة إلى الطلب فلا يشترط وجود إزدواجية التجريم للقيام بالحفظ.

4- أي دولة طرف تشترط وجود ازدواجية التجريم للاستجابة لطلب المساعدة يجوز لها في حالات الجرائم عدا المنصوص عليها في الفصل الثاني من هذه الاتفاقية، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة إذا كان هناك سبب للاعتقاد بأنه لن يتم تلبية شرط ازدواجية التجريم في وقت الكشف.

5- بالاضافة لذلك، يمكن رفض طلب الحفظ إذا :

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- إعتبار الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها.

6- حيثما تعتقد الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن التوفر المستقبلي للمعلومات أو سيهدد سرية تحقيقات الدولة الطرف الطالبة لها أو سلامتها فيجب عليها إعلام الدولة الطرف الطالبة لها لتحدد بعدها مدى إمكانية تنفيذ الطلب.

7- أي حفظ ناجم عن الاستجابة للطلب المذكور في الفقرة (1) يجب أن يكون لفترة لا تقل عن (60) يوماً من أجل تمكين الدولة الطرف الطالبة من تسليم طلب البحث أو الوصول أو الضبط أو التأمين أو الكشف للمعلومات. وبعد إستلام مثل هذا الطلب يجب الاستمرار بحفظ المعلومات حسب القرار الخاص بالطلب.

المادة الثامنة والثلاثون: الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة:

1 - حيثما تكتشف الدولة الطرف المطلوب منها – في سياق تنفيذ الطلب حسب المادة السابعة والثلاثين لحفظ معلومات تتبع المستخدمين الخاصة باتصالات معينة – بأن مزود خدمة في دولة أخرى قد اشترك في بث الاتصال فيجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدراً كافياً من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الاتصالات.

2 - يمكن تعليق كشف معلومات تتبع المستخدمين حسب الفقره (1) إذا:

أ - تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- اعتبرت الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سلامتها أو أمنها أو نظامها أو مصالحها .

المادة التاسعة والثلاثون: التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة:

1- يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة والثلاثين.
2- تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية.
3- تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضه للفقدان أو التعديل.

المادة الأربعون: الوصول إلى معلومات تقنية المعلومات عبر الحدود :

يجوز لأي دولة طر، وبدون الحصول على تفويض من دولة طرف أخرى:

1- أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات .
2- أن تصل أو تستقبل - من خلال تقنية المعلومات في إقليمها – معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.

المادة الحادية والأربعون: التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين:

1- على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينه في أقاليمها والتي تبث بواسطة تقنية المعلومات.
2- على كل دولة طرف توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المستخدمين لمثيلتها من القضايا الداخلية.

المادة الثانية والأربعون: التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى:

تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينه تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية .

المادة الثالثة والأربعون: جهاز متخصص:

1- تكفل كل دولة طرف، وفقاً للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات

المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة ويجب أن تشمل مثل هذه المساعدة تسهيل أو تنفيذ:

أ - توفير المشورة الفنية.

ب- حفظ المعلومات استناداً للمادتين السابعة والثلاثين والثامنة والثلاثين.

ج- جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين.

2- أ - يجب أن يكون لدى ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة.

ب- إذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزءاً من سلطات تلك الدولة الطرف المسؤولة عن المساعدة الثنائية الدولية فيجب على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة.

3- على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز المذكور أعلاه .

الفصل الخامس
أحكام ختامية

1- تعمل الجهات المختصة لدى الدول الأطراف على اتخاذ الإجراءات الداخلية اللازمة لوضع هذه الاتفاقية موضع التنفيذ.

2- تكون هذه الاتفاقية محلا للتصديق عليها أو قبولها أو إقرارها من الدول الموقعة، وتودع وثائق التصديق أو القبول أو الإقرار لدى الأمانة العامة لجامعة الدول العربية في موعد أقصاه ثلاثون يوما من تاريخ التصديق أو القبول أو الإقرار، وعلى الأمانة العامة إبلاغ سائر الدول الأعضاء والأمانة العامة لمجلس وزراء الداخلية العرب بكل إيداع لتلك الوثائق وتاريخه.

3- تسري هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية.

4- يجوز لأية دولة من دول الجامعة العربية غير الموقعة على هذه الاتفاقية أن تنضم إليها، وتعتبر الدولة طرفاً في هذه الاتفاقية بمجرد إيداع وثيقة التصديق أو القبول أو الإقرار أو الانضمام لدى الأمانة العامة لجامعة الدول العربية، ومضي ثلاثين يوما على تاريخ الإيداع.

5- مع مراعاة ما نصت عليه الفقرة (3) من المادة التاسعة عشرة، إذا تعارضت أحكام هذه الاتفاقية مع أحكام أية اتفاقية خاصة سابقة يطبق النص الأكثر تحقيقا لمكافحة جرائم تقنية المعلومات.

6- لا يجوز لأية دولة من الدول الأطراف أن تبدي أي تحفظ ينطوي على مخالفة لنصوص هذه الاتفاقية أو خروج على أهدافها.

7- يجوز للدولة الطرف أن تقترح تعديل أي نص من نصوص هذه الاتفاقية وتحيله إلى الأمين العام لجامعة الدول العربية الذي يقوم بإبلاغه إلى الدول الأطراف في الاتفاقية لاتخاذ قرار باعتماده بأغلبية ثلثي الدول الأطراف، ويصبح هذا التعديل نافذاً بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق أو القبول أو الإقرار من سبع دول أطراف لدى الأمانة العامة لجامعة الدول العربية.

8- يمكن لأية دولة طرف أن تنسحب من هذه الاتفاقية بناء على طلب كتابي ترسله إلى الأمين العام لجامعة الدول العربية.

ويرتب الانسحاب أثره بعد مضي ستة أشهر من تاريخ إرسال الطلب إلى الأمين العام لجامعة الدول العربية.

حررت هذه الاتفاقية باللغة العربية بمدينة القاهرة في جمهورية مصر العربية في 1432/1/15هـ ، الموافق 2010/12/21م من أصل واحد مودع بالأمانة العامة لجامعة الدول العربية (الأمانة الفنية لمجلس وزراء العدل العرب)، ونسخة مطابقة للأصل تسلم للأمانة العامة لمجلس وزراء الداخلية العرب، وتسلم كذلك نسخة مطابقة للأصل لكل دولة من الدول الأطراف.

وإثباتاً لما تقدم، قام أصحاب السمو والمعالي وزراء الداخلية والعدل العرب، بتوقيع هذه الاتفاقية، نيابة عن دولهم.

قائمة الدول العربية الموقعة والمصدقة على
الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

1- وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1432/1/15هـ الموافق 2010/12/21م.
2- تسرى هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية بموجب الفقرة (3) من الاحكام الختامة للاتفاقية.

الـــــدولة	تاريخ التوقيع	تاريخ التصديق أو القبول أو الإقرار
المملكة الأردنية الهاشمية	2010/12/21	2013/1/8
دولة الإمارات العربية المتحدة	2010/12/21	2011/9/21
مملكة البحرين	2010/12/21	
الجمهورية التونسية	2010/12/21	
الجمهورية الجزائرية الديمقراطية الشعبية	2010/12/21	
جمهورية جيبوتي		
المملكة العربية السعودية	2010/12/21	
جمهورية السودان	2010/12/21	2013/7/15
الجمهورية العربية السورية	2010/12/21	
جمهورية الصومال		
جمهورية العراق	2010/12/21	
سلطنة عمان	2012/2/15	
دولة فلسطين	2010/12/21	2013/5/21
دولة قطر	2010/12/21	2012/5/24
جمهورية القمر المتحدة		
دولة الكويت	2010/12/21	2013/9/5
الجمهورية اللبنانية		
دولة ليبيا	2010/12/21	
جمهورية مصر العربية	2010/12/21	
المملكة المغربية	2010/12/21	
الجمهورية الإسلامية الموريتانية	2010/12/21	
الجمهورية اليمنية	2010/12/21	

الجريمة الإلكترونية في الفقه الجنائي الإسلامي

The Electronic Crime in the Islamic Criminal Jurisprudence

Abstract:

The technicality of information and modern mass media have become Part of the human behavior and system of values to all members of society including the Muslim community. Moreover, the use of technology has become one of the most important requirements of life and an indication of the social consciousness as it allows a wider choice in dealing with all areas of daily life. Nevertheless, the misuse of these modern technologies such as the internet and the computers, the speed of deployment and lack of control raises concerns in many cases. Therefore, this is due to the absence of religious faith and an effective guidance that might overcome the negative effects Which resulted in the emergence of deviant behavior which in turn influenced the security system in the community.

Hence, the importance of singling out a specialized scientific Jurisprudential investigation has been found fundamental. The research was conducted to show the legitimate aspects of the cyber crime phenomenon in the Islamic criminal jurisprudence. It is an attempt to shed light and determine the size and style of the most updated crimes with an indication of their seriousness on public and private interests. This is for the purpose of laying down the outlines that identify how we could fight and reduce them with reference to the Islamic law. This latter is only lacking to exert more diligence, insight and permanent attendance at any emergency; and the discovery of the privacy for every time and place and the appropriate estimation for the rulings, procedures and measures.